Grenze International Journal of Engineering and Technology, Jan Issue

Secure Messaging using Blockchain Technology

Ruby D[1] and Hrishikesh Magadum[2]
[1-2]Vellore Institute of Technology/School of Computer Science and Engineering, Vellore, India
Email: ruby.d@vit.ac.in, hrishikesh.magadum2019@vitstudent.ac.in

***Abstract*— All messaging platforms rely on a centralized server which has the vulnerability of getting hacked by outside agencies and posing risk to private data. Authentication between users is an important asset in electronic messaging today, which is one of the most widely used network applications. By replacing the need for reliable mediators, blockchain technology overcomes these threats and allows for a reduction in power-intensive operations. In this work, we propose a blockchain-based solution for secure messaging. Blockchain-based communication can increase communication effectiveness and security, and this paper proposes the creation of a blockchain-based messaging model that will improve the performance and security of blockchain-recorded data, with a smart contract to verify ownership. The system is still fully distributed and allows users to exchange messages securely. This paper has tried to implement a blockchain with a few users and implemented secure end-to-end encryption using the SHA-256 algorithm and multiple crypto techniques so that messages cannot be vulnerable.**

I. INTRODUCTION

In today's world, most methods of communication are ruled by centralized messaging services, like iMessage, Facebook Messenger, WhatsApp, and GroupMe [3]. With Block Chain technology we hope to solve several issues with these centralized messaging services. The lack of interoperability asynchronization in communication with the same individual across numerous platforms, as well as a lack of data ownership around the privacy and content of the messages, are becoming increasingly typical difficulties that result from these centralized services. Users are required to create a separate account with each centralized messaging provider (e.g., Facebook, Apple, Google), implying that messaging services have ultimate control over the user's data. PKI is a crucial aspect of resolving network purchases since it ensures that a signed certificate is authenticated by a certifying authority (CA) [5]. A new notion known as his trust's web name PKI is used by the Pretty Good Privacy (PGP) encryption system to provide encryption, authentication, and a web of hope with peer-to-peer identity verification. Certificates allow you to execute cryptographic tasks like encryption and digital signature by authorizing the public keys. PKI has one point of failure since authentication is in the middle [5]. The purpose of blockchain technology is to make transactions more secure. Blockchain technology, which relies on cryptography to provide resistance to interference, is a viable solution for achieving data integrity. To ensure that transactions are secure, all network participants must agree, and earlier records cannot be modified [20]. If someone wants to replace prior records, they should use a very high cost. Terminal attackers will have to get simultaneous access to all computers on this network hosting a blockchain database, which is nearly difficult. A block is added to the Blockchain via the mining process after it is complete. When a new block is added to the Blockchain, the Proof of Work (PoW) cryptographic puzzle that the miners are attempting to solve is launched [21]. Bitcoin is built on a system of trust that is assigned to a specific location. Blockchain databases can't be hacked, changed, or erased. Consistency when the chain is lengthy, the data in this blockchain is incredibly secure.

Grenze ID: 01.GIJET.10.1.512_2

A. Blockchain

A distributed database known as a blockchain is a public ledger of all transactions made and shared among participating organizations that tolerate record inaccuracies. The majority of the system's participants verify each transaction on the public ledger [1]. Blockchain is a technique that uses a combination of encryption and consistency to increase data integrity. As a result, the server has no single point of control. Blocks of data are used to store information. Each block is secured and contains a transaction, timestamp, and link to the preceding block [10]. As a result, it is safe because:

- *Key public infrastructure*: Stores and exchanges data securely using public/private key encryption and data hashing.
- *Distributed ledgers*: Eliminates a single point of failure by eliminating the need for a central authority to hold and manage data.
- *Peer-to-Peer Network*: Communication is based on P2P network structures and low-level feature acquisition.
- *Cryptography*: A number of cryptographic techniques, such as hash works, Merkle trees, and public and private keys, are used in blockchain [25]. It is difficult to change the blockchain and make modifications; nonetheless, it is critical to succeeding in simultaneous attacks on more than 51% of members.
- *Consensus Algorithm*: A set of rules that nodes in a network follow to validate the integrity of a distributed ledger. Consensus algorithms are used to achieve dependability in systems with a large number of faulty nodes [21].
- *Transparency*: Anyone with access to the system can see every transaction. The input is immediately rejected if it cannot be confirmed. As a result, the data is entirely transparent. Each blockchain node is identified by a unique address.

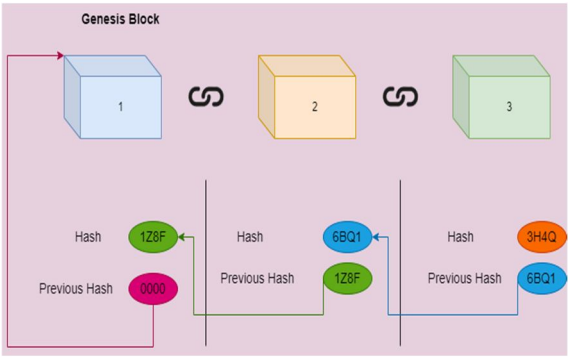

Fig.1.1 Idea of Blockchain

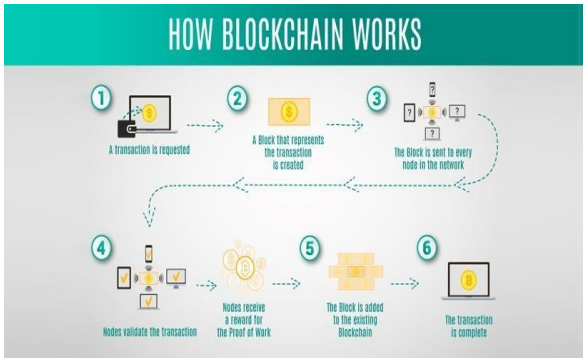

Fig. 1.2 Working of Blockchain

Fig.1.1 and Fig 1.2 depicts the idea and working of Blockchain. The various steps in the adding of a new block every time is depicted in the above picture-

Scope of Blockchain Messaging- Blockchain decentralizes data and allows only authorized individuals to access any set of data [2]. Each transaction is validated by 51% of the users of the people participating in the blockchain, the issue of illegal transactions or transactions exceeding limits does not possess a big threat to this technology [6]. Each valid transaction is monitored by each and every member and invalid transactions are never written in the blockchain. The scope of this technology in the future is very much realistic and several prototypes have been made recently using this technology but have to be fully utilized by ordinary people and big level organizations.

II. Literature Survey

Khacef, Kahina, and Pujolle in [1] suggested an idea to secure Peer-to-Peer communication based on Blockchain. The proposed methodology involves using the blockchain to verify the identity of the sender and establish trust amongst users in order to send secure messages. Such a system is composed of a centralized blockchain System using smart contracts and a public key encryption algorithm which is one of the famous data-securing methods present. Using a smart contract to authenticate identities and their associated public keys, as well as to validate the user's certificate, the author of this paper explained why blockchain technologies make communications more secure. They also proposed a blockchain-based messaging model to ensure the performance and security of data stored on the blockchain. The system is entirely decentralized.

Suman Kumar Das in [2], the viability and benefits of blockchain technology in chat applications were investigated, and a blockchain-based messaging system was developed. This paper proposed a blockchain-based

system to counter and fix concerns with messaging systems, as well as to assist users in securely exchanging messages and information. This author has demonstrated how confidential and private communications are viewable at the chat server's processing or computing end. The authors also explained and demonstrated how a blockchain-based chat application using the whisper protocol in peer-to-peer mode can allow users safely exchange information.

In [3] the authors have formulated a Blockchain-Enabled End-to-End Encryption for Instant Messaging Applications. The intended blockchain-backed E2EE system attempts to guarantee true privacy without the need to share private keys with other parties such as IM servers. The key feature of this paper was that backup decryption keys are also stored on the IM server and the end-to-end encryption/decryption on the mechanism is controlled by the service providers themselves.

Luo Kan and the authors in [4], the interactive multiple blockchain architecture was introduced in this paper as a new component-based framework for transferring information across arbitrary blockchain systems. For inter-blockchain communication, the paper's architecture creates a dynamic network of multi-chains. For routing management and message transfer, the authors presented an inter-blockchain connection paradigm. The offered protocols also give transactions atomicity and consistency in a crossing-chain scenario. Last but not least, the results of the experiment based on a network of private multiple blockchain systems show that the throughput improves with the number of chains running concurrently.

The authors of [7] provide a thorough technical and practical analysis of blockchain-enabled smart contracts. They categorized the included research papers, analyzed the studies that have been done using smart contracts, and created a taxonomy of blockchain-enabled smart contract solutions. The study revealed a number of challenges and unresolved issues that future studies should address. This study provides information assistance to participants interested in the study of smart contracts.

The research in [9] looks into the several ways that the term "decentralization" is used in relation to distributed ledgers and blockchains. The study aims to capture the rigorous cross-domain knowledge of decentralization and its important characteristics as well as to map the parallels and differences between decentralization and other closely related concepts, such as distribution, disintermediation, and peer-to-peer (P2P). The authors present their findings from a systematic review, outline a framework for understanding decentralization enabled by blockchain technology, offer a definition, and suggest new lines of inquiry for future human-centric studies on distributed ledger technologies and the creation of decentralized ecosystems.

In [20], the article's writers made a case for a private, decentralized messaging system and developed a proof-of-concept utilizing Whisper and the Ethereum platform. Even in the face of an adversary in control of the majority of the network, the application may send end-to-end encrypted messages while ensuring that the sender and recipient's identities are kept secret. Discussions include the employed encryption technique, the application's defense against several threats, and network traffic analysis.

In order to avoid personal data loss, a simulation messaging platform built on the Bitcoin protocol is suggested in this paper [22]. The chosen method makes use of the blockchain's decentralized data storage and offers a private exchange of encrypted messages and photos. The suggested UNCUFFED system, which supports two user groups, the Miners and the Clients, prevents attempts to get valuable data. Clients communicate messages outside of the platform, while Miners get incentives as active blockchain users.

III. Objective

The main aim of this blockchain-based chatting application is to successfully send and receive messages between any two users as well as send and receive blockchain cryptocurrency between two users. This paper also demonstrates how each transaction gets validated by smart contracts and added to the blockchain. The expected results also consist of transaction logs, blocks mined, and smart contracts that are used as a consensus for approval of any transaction.

IV. System Design

The developed system *is secure messaging using blockchain technologies*. Blockchain's main motive is to decentralize the system and completely eradicate the issue of trusting a central authority. The concept of blockchain refers to a series of blocks linked together. A data structure that includes information and some properties is known as a block. The developed system consists of 10 users, each user having a hexadecimal address. New users can be added via a function that validates the user by the consensus algorithm where each new user will have a private key and a public key. Each user is interconnected to each other via the network. The objective of the work is to

ensure communication security between network elements. The presented method involves using the blockchain to verify a user's identity and establish trust amongst users in order to send secure messages. Every user must only interact with other users whose identities have been verified by the consensus mechanism, and all other interactions must be regarded as malevolent. Each user who interacts with others via the system should verify their identity as well as their public key and deposit it on the blockchain.

A. Smart Contract

A smart contract is a piece of code that is stored and run on a blockchain. Once a smart contract is launched, users are unable to make changes because the contract has already been delivered and validated [2], [7]. A transaction can be sent to a contact's address, and it will be completed. The next two steps are blockchain registration and smart contract-based verification.

B. Send/Receive

Following the successful completion of mutual authentication, Alice creates a shared secret using both her private key and Bob's public key. The shared secret can be created using the Elliptic curve-Diffie-Hellman (ECDH) technique to encrypt the Message [3]. After being generated, the shared key is subsequently used to symmetrically encrypt messages.

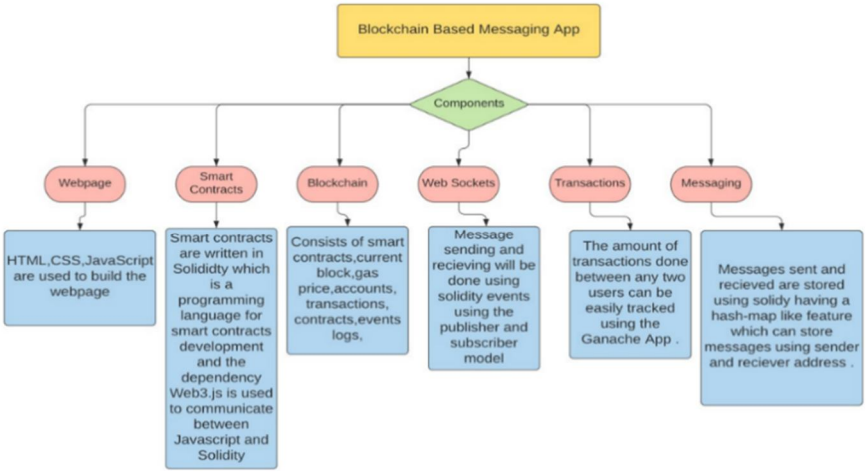

Fig. 4.1 Architectural diagram based on various components of the implementation

V. IMPLEMENTATION

The execution of the system and agreements between different users depend on the smart contract. The agreement reached by the nodes to authenticate the certificates of persons can be implemented via smart contracts by developing scripts that run on the blockchain, which can then be utilized to create the suggested system [7]. Every time the contract is invoked, a new update to its state is made on the blockchain. The smart contract checks the sender's identity and the key associated with it, which was previously saved on the blockchain, before sending or receiving the message. The timestamp is then checked for legitimacy. Finally, the signature is checked by the smart contract. Solidity is capable of creating a smart contract**.** Web3 is a library that helps map the Solidity programming language to simple Javascript functions. All changes made in the chat application are recorded in the Ganache App. To have live messaging we use React Javascript which is a library in Javascript used to handle and trigger live data modifications without reloading the web page. Websockets, help us to run 2 userson 2 different servers and keep their ports open to listen to various events between them so that live exchange of messages can be done between the participants of the blockchain.

A. Connecting Metamask to browser

First and foremost, we must set up Metamask. Metamask is a browser extension that allows you to set your personal ledger wallets to store tokens that will be used to interact with our future blockchain. We build a new network by clicking custom RPC at the top right of the extension after installing the plugin on the shop. The plugin is then linked to the information that was used in our project.

B. On the Blockchain side

The web app includes the following features:

- Connect to all of Ganache's accessible wallet addresses.
- Transfer messages between these addresses.
- Save all messages in the smart contract so that they can be retrieved when the page is reloaded.
- Watch the state of the blockchain in real-time as transactions are completed.

C. Connecting Ganache Wallets to the browser

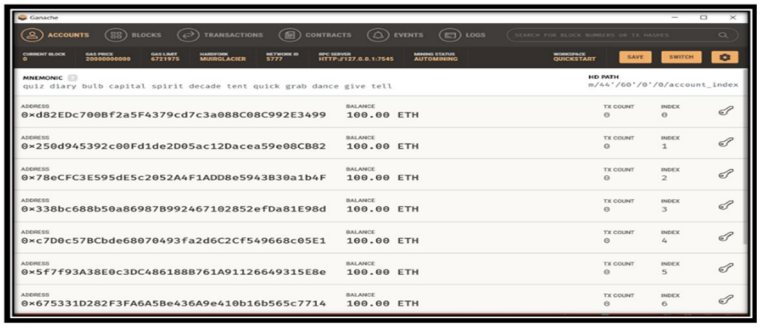

Fig. 3.6 Fetching user accounts from the Blockchain. This is the Ganache App where Blockchain-related information is stored.

D. Sending Messages

To send messages using blockchain technology can be done with the help of Solidity events. A Solidity event is similar to software architectures like MVM or Block. In our scenario, a client is listening for incomingdata after subscribing to a type of event. Then you can send out an event to all of your clients. Each event on the blockchain consumes some gas, hence it has a cost.

E. Storing messages in the blockchain

The mapping object in Solidity is a hash map-like data structure. Two nested mapping objects will be used: The conversation is a mapping of the sender's address to the receiver's address and then to a list of messages.So, if we only have the two addresses, we can now retrieve the messages. The Message structure from the address is utilized to determine whether the messages were sent or received from each of the two addresses.

F. Sending Ether

Ether is the cryptocurrency of this app and we can send a definite amount of cryptocurrency between 2 users. Each user has a limited amount of currency to spend or share. Solidity makes sending ether tokens from one address to another a breeze. The function must be "payable" as it has to send tokens. Msg. value specifies the amount of ether to send.

VI. Results And Discussions

A. Description

The project is a real-time communication application based on blockchain and contains only the features to send and receive messages and ether, which is the cryptocurrency of this chat application. The blockchain contains 10 users initially for convenience and ease of testing. Each of the 10 users will have a unique address so that messages are sent to the respective recipient only and the sender and receiver addresses can be tracked in the block for any reference the blockchain interface called Ganache is responsible for this action. For every message the user does, his transaction count increases by one. Adding to that every user has a fixed amount of cryptocurrency allotted to him using which he/she can send money to other people. For this blockchain, the cryptocurrency used is ether (ETH). Each user has a unique ID associated with him and each user has a transaction count on his name. So test data set consists of 10 users with 100 ETH in their wallet and the transaction count is set to 0 for every user.

B. Full Demonstration of the Blockchain Chatting App

The highlighted addresses are the accounts/users who took part in the sending/receiving of messages. Initially when no messages are sent the number of blocks in the Blockchain remains unchanged as no transaction took place. The state of the sender and receiver side is illustrated in the following diagrams-

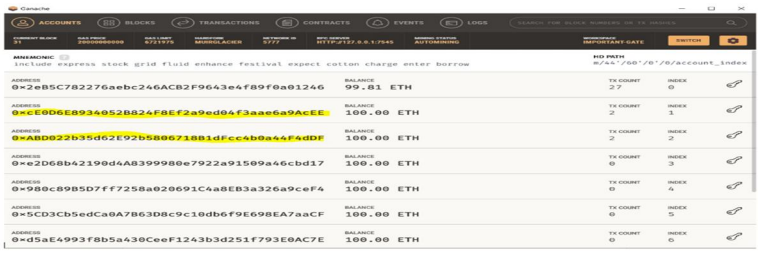

Fig.3.7 The Ganache UI for the users and their details

Sender Side Address-0xcE0D6E8934052B824F8Ef2a9ed04f3aae6a9AcEE
Receiver Side Address-0xABD022b35d62E92b5806718B1dFcc4b0a44F4dDF
Message sent from address-0xcE0D6E8934052B824F8Ef2a9ed04f3aae6a9AcEE to address 0xABD022b35d62E92b5806718B1dFcc4b0a44F4dDF respectively are considered as a valid transaction and stored in the Blockchain.

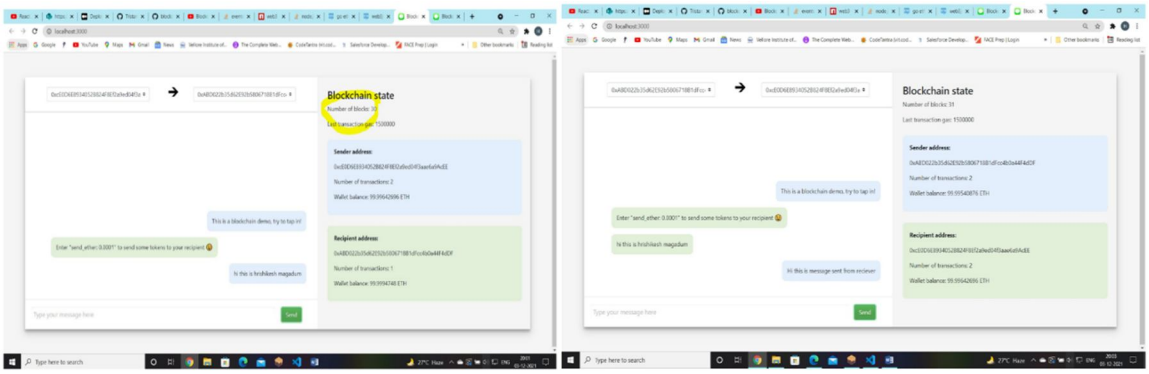

Fig.3.8 Blockchain state

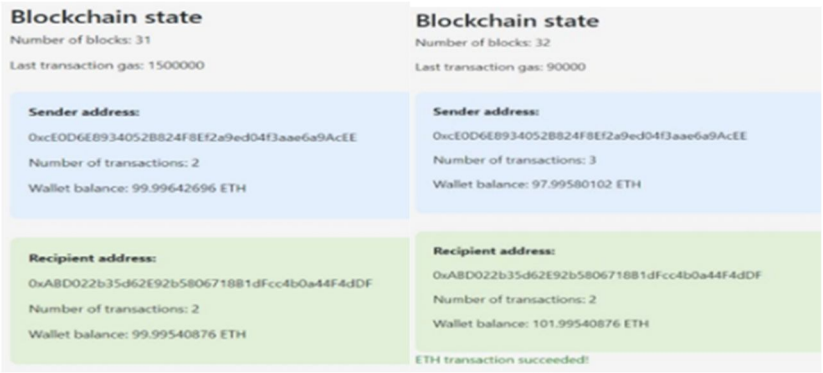

Fig.3.8 when we send a message, the number of blocks increases by 1 and so does thenumber of transactions. On the Ganache app, we can see the details about the users, their transaction count as well as the wallet money they have. Sending Cryptocurrency ether between 2 accounts is successful and is reflected in the wallet balance.

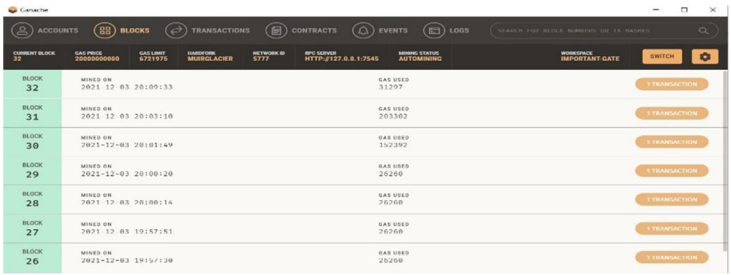

Fig.3.9 on the Ganache App, we can see all the details of the blocks created as a consequence of communication or money transferred between users.

Fig.3.10 The transactions that took place are all stored in the blockchain permanently and are immutable in nature.

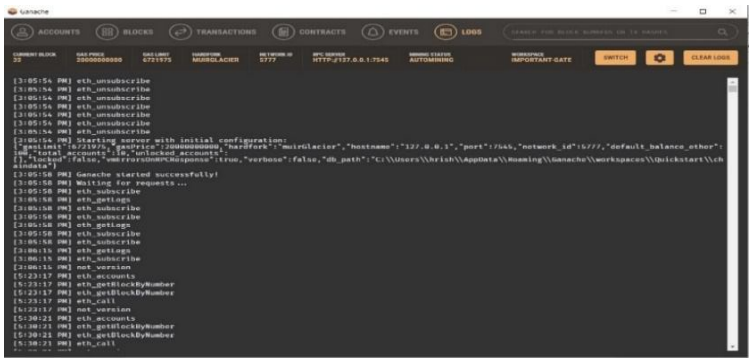

Fig.3.11 Logs help us detect user activity and find potential transactions that might be considered illegal. The exact timestamp is recorded to provide a transparent history of all the transactions to all the users present in the blockchain.

VII. Conclusion

This model gave us a clear idea of how a blockchain worked in real life and how it can be beneficial in future implementations as a predominant technology. This technology can be used to replace the current centralized communication platforms as well as give us a major upgrade in the process of decentralization without any compromise of security. Blockchain technologies are very secure as it is difficult to know the hash of a block and when too many blocks get added, the permutations to find the hash values become so large that it becomes almost impossible to determine the value of the hash. So any intruder or a hacker or maybe even an organization willing to attack an existing blockchain may not be able to do it irrespective of how many computing sources they add on. The issues of data leakage, man-in-the-middle attacks, leaking personal chats, access to personal documents, and many more issues will be resolved if blockchain technology is incorporated into our communication platforms. The disadvantage of blockchain technology is that maintaining a blockchain is very difficult as the number of participants increases. To maintain the blockchain the amount of energy one has to spend goes on increasing. Distributed computing can help us to maintain the block. Just like we pay for communicating through mobile, we can implement a system where any user has to pay a fixed amount to do a transaction in the block and the fee collected from him will be used to maintain the blockchain. So to conclude, blockchain is a more trustable source rather than centralized systems exist and if implemented correctly would be a great technology of the future.

Future Work

We can use the popular RSA algorithm to encrypt messages. It is similar to end-to-end encryption but the difference is that the key is more difficult to hack and will add another layer of security to the Blockchain Chat App. To share and store data in a distributed file system, the IPFS protocol can be included. It employs context addressing to uniquely identify every single file in a global namespace connecting all blockchain users, which are the computing devices that help run the blockchain. Optimization of the gas consumption in a smart contract. The smart contract requires a specific amount of gas and be very costly at times, but with a certain type of approach, the gas consumption can be brought down which will be very beneficial for the Application to be maintained from a financial point of view.

REFERENCES

[1] K. Khacef and G. Pujolle, "Secure peer-to-peer communication based on blockchain," in Advances in Intelligent Systems and Computing, vol. 927, Cham: Springer International Publishing, 2019, pp. 662–672.

[2] S. K. Das, "Secure messaging platform using blockchain technology," Ijres.org. [Online]. Available: https://ijres.org/papers/Volume-8/Issue-12/3/E0812032630.pdf. [Accessed: 24-Jun-2022].

[3] R. Singh, A. N. S. Chauhan, and H. Tewari, "Blockchain-enabled end-to-end encryption for instant messaging applications," arXiv [cs.CR], 2021.

[4] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A Multiple Blockchains Architecture on Inter-Blockchain Communication," in 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, pp. 139–145.

[5] N. Unger et al., "SoK: Secure Messaging," in 2015 IEEE Symposium on Security and Privacy, 2015, pp. 232–249.

[6] A.P. Takale, C. V. Vaidya, S. S. Kolekar, and U. G. Student, "Decentralized Chat Application using Blockchain Technology," Ijream.org. [Online]. Available: https://www.ijream.org/papers/CTRD2018026.pdf. [Accessed: 24-Jun-2022].

[7] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018.

[8] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of Blockchain technology in live stream video transmissions and telecommunications," Int. j. e-collab., vol. 16, no. 1, pp. 16–32, 2020.

[9] M. R. Hoffman, L.-D. Ibáñez, and E. Simperl, "Scholarly publishing on the blockchain – from smart papers to smart informetrics," Data sci., vol. 2, no. 1–2, pp. 291–310, 2019.

[10] G. Wang, S. Zhang, T. Yu, and Y. Ning, "A systematic overview of blockchain research," J. Syst. Sci. Inf., vol. 9, no. 3, pp. 205–238, 2021.

[11] A. Qasse, M. A. Talib, and Q. Nasir, "Inter Blockchain Communication: A Survey," in Proceedings of the ArabWIC 6th Annual International Conference Research Track on - ArabWIC, 2019.

[12] X. Xiao, Z. Yu, K. Xie, S. Guo, A. Xiong, and Y. Yan, "A Multi-blockchain Architecture Supporting Cross-Blockchain Communication," in Communications in Computer and Information Science, Singapore: Springer Singapore, 2020, pp. 592–603.

[13] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," Electronics (Basel), vol. 9, no. 9, p. 1338, 2020.

[14] Li, G. Liang, and T. Liu, "A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication," KSII Trans. Internet Inf. Syst, vol. 11, no. 8, pp. 3766–3788, 2017.

[15] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," IEEE Commun. Surv. Tutor., vol. 22, no. 2, pp. 1392–1431, 2020.

[16] A. Kapitonov, I. Berman, S. Lonshakov, and A. Krupenkin, "Blockchain based protocol for economical communication in industry 4.0," in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018.

[17] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards Blockchain Interoperability," in Business Process Management: Blockchain and Central and Eastern Europe Forum, Cham: Springer International Publishing, 2019, pp. 3–10.

[18] H. Wang, Y. Cen, and X. Li, "Blockchain Router: A Cross-Chain Communication Protocol," in Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, 2017.

[19] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," IEEE J. Biomed. Health Inform., vol. 24, no. 8, pp. 2146–2156, 2020.

[20] M. Abdulaziz, D. Culha, and A. Yazici, "A decentralized application for secure messaging in a trustless environment," in 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), 2018.

[21] Subbiah, "The Age of blockchain: A Collection of articles," IndraStra Global, 2018.

[22] U. P. Ellewala, W. D. H. U. Amarasena, H. V. S. Lakmali, L. M. K. Senanayaka, and A. N. Senarathne, "Secure messaging platform based on blockchain," in 2020 2nd International Conference on Advancements in Computing (ICAC), 2020.

[23] N. Unger and I. Goldberg, "Deniable key exchanges for secure messaging," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15, 2015.

[24] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," IEEE Internet Things J., vol. 8, no. 4, pp. 2276–2288, 2021.

[25] R. A. Saritekin, E. Karabacak, Z. Durgay, and E. Karaarslan, "Blockchain based secure communication application proposal: Cryptouch," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018.

[26] D. Li, W. Liu, L. Deng, and B. Qin, "Design of multimedia blockchain privacy protection system based on distributed trusted communication," Trans. emerg. telecommun. technol., vol. 32, no. 2, 2021.

[27] H. Zhao, M. Zhang, S. Wang, E. Li, Z. Guo, and D. Sun, "Security risk and response analysis of typical application architecture of information and communication blockchain," Neural Comput. Appl., vol. 33, no. 13, pp. 7661–7671, 2021.