# A Secured Peer-to-Peer Messaging System Based on Blockchain

**Conference Paper** · April 2022

DOI: 10.1109/ICIEM54221.2022.9853040



**7 authors**, including:

Shamim Ahmed
Bangladesh University of Business and Technology
**29** PUBLICATIONS **225** CITATIONS
SEE PROFILE

Milon Biswas
University of Alabama at Birmingham
**78** PUBLICATIONS **792** CITATIONS
SEE PROFILE

Md.Julkar Nayeen Mahi
Daffodil International University
**43** PUBLICATIONS **404** CITATIONS
SEE PROFILE

Md. Ashraful Islam
Bangladesh University of Business and Technology
**7** PUBLICATIONS **52** CITATIONS
SEE PROFILE

# A Secured Peer-to-Peer Messaging System Based on Blockchain

Shamim Ahmed*, Milon Biswas†, Md. Hasanuzzaman‡, Md. Julkar Nayeen Mahi§,
Md. Ashraful Islam¶, Sudipto Chaki‖, Loveleen Gaur**
Bangladesh University of Business and Technology, Dhaka, Bangladesh.*†‡¶‖
Daffodil International University§
Amity University, India**
Email: shamim.6feb@gmail.com*, milon@ieee.org†, hasan.mon98@gmail.com‡, mahi.1992@gmail.com§,
ashacse42@gmail.com¶, sudiptochakibd@gmail.com‖, lgaur@amity.edu**

***Abstract*—Nowadays, the messaging system is one of the most popular mobile applications, and therefore the authentication between clients is essential. Various kinds of such mobile applications are using encryption-based security protocols, but they are facing many security threat issues. It clearly defines the necessity for a trustful security procedure. Therefore, a blockchain-based messaging system could be an alternative to this problem. That is why, we have developed a secured peer-to-peer messaging system supported by blockchain. This proposed mechanism provides data security among the users. In a blockchain-based framework, all the information can be verified and controlled automatically and all the transactions are recorded that have been created already. In our paper, we have explained how the users can communicate through a blockchain-based messaging system that can maintain a secured network. We explored why blockchain would improve communication security in this post, and we proposed a model architecture for blockchain-based messaging that retains the performance and security of data stored on the blockchain. Our proposed architecture is completely decentralized and enables users to send and receive messages in an acceptable and secure manner.**

***Index Terms*—Message, Blockchain, Proof of Work (PoW), Security, Hash Function.**

## I. Introduction

Nowadays, companies are facing a new challenge in data management and security issues. To solve this problem, blockchain based technology emerges as a possible way to allow transactions to be carried out and verified on the network instantly without a central authority. Known only for the technology that underlies bitcoin, a digital currency, blockchain has acquired a replacement identity within companies. Today, several growing companies in many major financial institutions and industries are experimenting with a distributed transparent technology securely and transparently as it tracks asset ownership digitally. This can accelerate transactions and reduce costs while decreasing the risk of fraud. As our lives grow more positive about digital and web services, the problem of retaining total autonomy and protection when completely exchanging identity content or data is increasingly growing. What was once our power and influence can now be quickly stolen and sent to a plethora of institutions all over the world. Identity fraud, leaked databases, and compromised accounts are highlighting the rising challenge of an evolved society with obsolete identity-based technology innovations. Current approaches rely on vulnerable mechanisms that swap and store shared hidden passwords. Using digital signatures that support public-key cryptography, blockchain based authentication systems have irrefutable biometric authentication. In this article, we suggested a forum for safely and privately sending messages over the blockchain. Authentication between users is a critical property in today's world since messaging is the most commonly used network technology. The public key infrastructure (PKI) and Secure/Multipurpose Internet Mail Extensions (S/MIME) email encryption protocols [1] are the most commonly used methods for securing this property. However, they are vulnerable to a variety of security attacks, including the man in the middle (MITM) attack and the EFAIL attack. Blockchain is a cutting-edge technology that eliminates the need for trusted intermediaries and helps us to decentralize confidential operations while retaining a high degree of protection. The blockchain is a distributed ledger that is open to all of any nodes on the network and keeps track of all previous transactions. Our research aims to develop a decentralized messaging system based on blockchain technology. In this paper, we've discussed why blockchain is more stable and how a smart contract will ensure the integrity of information stored on the blockchain.

The key contribution of this proposed framework is highlighted in the followings.

1) Proposed blockchain based P2P messaging framework provides a secured path for transmitting and receiving messages.
2) A verification of proof of work algorithm has been implemented.

The rest of this paper is outlined in the following manner. Section **II** describes some related works that have already been proposed by different authors. Section **III** discusses the necessary parameters for designing our framework. Section **IV** describes our proposed P2P framework for a secured messaging system. Lastly, we have briefly discussed the conclusion and future works in this field of research in section **V**.

## II. Related Research

As our lives become more reliant on websites and streaming platforms, the issue of full control and protection while sharing digital identity, information, and data is becoming more urgent. The Public Key Infrastructure (PKI) [1] is a critical component of network authentication resolution since it ensures the trustworthiness of certificates signed by a Certificate Authority (CA) [2]. PKI is used to guarantee secrecy through encryption, verification by signature, and Web of Trust by validating peer identity in an analog concept to the Very Good Privacy (PGP) encryption scheme known as the Web of Trust. Popular public keys are authenticated with certificates, allowing them to execute cryptographic operations like encryption and digital signatures. Individual error sources

result from the PKI's centralization of authentication and identity checking. Blockchain technologies aimed to improve transaction security [3]. Bitmessage [4] is a popular decentralized messaging system that allows users to send and receive messages while preventing eavesdropping. The blockchain flooding amplification method and asymmetric encryption algorithm are used by Bitmessage to achieve anonymity and safety. The blockchain has recently piqued the interest of scholars, and it has enormous promise in a variety of fields. The blockchain is a decentralized and distributed networking paradigm that underpins the cryptocurrency Bitcoin [5] and offers data storage and privacy in peer-to-peer (P2P) networks. Since any vehicle can access the history of event details inside the public blockchain, blockchain is also used to handle the simple truth of vehicle data in VANET. In terms of security issues, blockchain provides a reliable decentralized platform [6] to contract anonymously while keeping all the necessary data in safeguard. During a financial transaction, it is important to provide a safe channel. That is why blockchain-based security management is getting popular day by day. In near future, all kinds of financial deals may be validated through this emerging technology.

In the recent past, many industries involved in product developments have shifted their data and stored files to a decentralized network [7] in terms of facilitating the data exchange rate between different wings of an organization. This trend has a big impact on industrial revolution 4.0. It has been successfully run by many industries and they are growing fast as a whole by exchanging information more securely in a systematic process. A human-computer interaction (HCI) based [8] communication network is built to exchange messages securely through the network where both the software and hardware combinations are effectively utilized. This framework was used to assist disabled persons so that they can communicate in a more secure medium. Yi [8] proposed a combined framework for instant messaging [9] where both blockchain and machine learning techniques are used as a whole. During online shopping, to provide secure communication [10]–[12] between a buyer [13] and seller, this proposed framework [14] was tested. As traditional social media applications are not decentralized [15], this technique [16] has helped to build a more secured network [17] over communication periods.

## III. System Design Parameters

Blockchain is a state-of-the-art technology that comes out of these threats and makes it possible to disseminate sensitive services while ensuring a high level of security. Reliable mediators are not required. The purpose of our work is to suggest a secured messaging solution that supports blockchain technology. The system is completely scalable and allows users to exchange messages securely. The parameters that control the system designing part are discussed in the following subsections.

### A. Design as an Artifact

The central premise of this research is that the design of the modified distribution data system is supported by a network of objects and thus blockchain technology [18]–[20] supports its infrastructure. This new system eliminates the need for a trustworthy central organization. Data communication takes on myriad forms and requires robust support systems to ensure security and continuous maintenance. Often, it is difficult to distinguish this from different systems or existing APIs due to competing interests and a lack of security protocols. Some companies are using the blockchain to create a much better communication infrastructure. In their view, this indicates the creation of a secure ecosystem for messaging services, while expecting the same security guarantees that the underlying technology enables. The blockchain [21] is the ideal solution because it stores data in all network networks and, as distributed digital communication, makes it easier to work securely [22].

### B. Scalability

A very large number of people can participate in the messaging program, which is a combination of the world, with a huge flow of newly developed information and a difficult time. All of this data is not well managed by current management systems because proper data management system is scarce. Blockchain can make a significant contribution to marketing by providing comprehensive and integrated data retrieval to all parties involved.

### C. Consensus

Blockchain platforms have selected technologies that ensure the stability of the data along with the new ledger known as the contract. The real measure of the agreement is to maintain a common agreement between the websites and all the marketing information that is transmitted. Today, blockchain platforms support different types of multi-agreement tools based on standard ledger entry steps. The sign is usually public or private, and common consent algorithms are a sign of service and evidence of coherence. Consensus algorithms form the basis of blockchain trust and consensus of all sites, in what is commonly known terms like "mining".

### D. Security and Privacy

Unlike messaging systems, where any legitimate data may be hijacked, blockchains provide a substantial contribution to privacy. Not only can blockchain devices deliver an outstanding experience, but user privacy is also greatly appreciated. Public blockchains provide their users with a pseudonym, meaning that each user is in a domain-friendly environment via a newly formed address without divulging their genuine identity. Permission and personal blockchains can also provide complete network anonymity in the following ways.

- **Confidentiality:** Peer to peer encryption between endpoints can be set once the communication channel between users has been protected, and only authorized users will have access to the messages transmitted.
- **Authentication:** The blockchain checks the legitimacy of a signature before storing it. No one else may alter or modify the signed agreement or change the exchanged message while it is in transit over the network. Each user on the blockchain has a unique certificate. The certificate is used by the smart contract to verify the user's identity.
- **Reliability:** It is difficult to turn off all blockchain computers at the same time. As a consequence, this database is always available and operational.

## IV. Our Blockchain-Based Messaging System

Our system enables its users to transfer information and prove the defining attributes and status with a great deal of reliability. Usually, a messaging system is threatened by

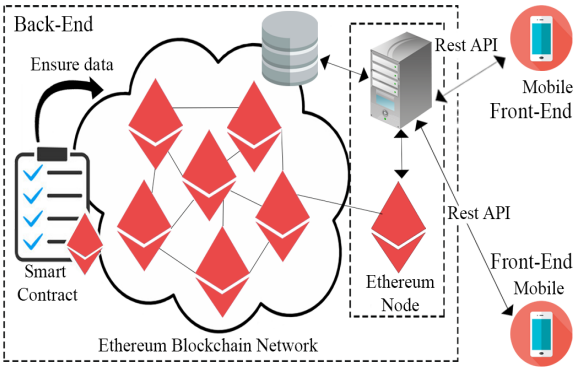


Fig. 1. Blockchain intregrated architecture for peer to peer messaging system.

different types of frequent and continuous threats with potentially serious consequences. These illegal activities include: making fake messages with passive or harmful components, stealing and diversifying legitimately, and illegal schemes like changing the message. A comprehensive security solution, which is the goal of our proposed framework will do much to mitigate these risks. Our proposed blockchain integrated P2P messainging architecture system is shown in Fig. 1. The flow diagram shown in Fig. 2 illustrates the validation part of our proposed system. If the validation is correct, the message is sent to the destination otherwise the sending request is discarded by the system.

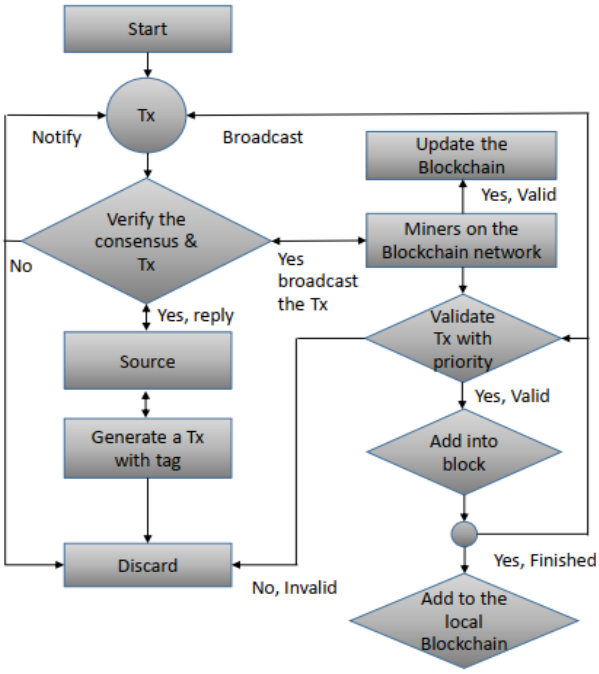


Fig. 2. P2P message flowchart in the transaction and consensus processing.

### A. Proof of Work (PoW)

The sign-of-service can be a way to achieve global consensus on the actual blockchain. Since all nodes have a blockchain image, each node must agree on what conditions indicate how many attempts have been completed to analyze the transaction. Proof of service is a protocol with the primary purpose of preventing cyber-attacks such as distributed redundancy (DDoS) attacks, which aim to deplete the computer system resources by sending multiple requests. To establish ownership, the user must supply her public key as well as her signature. To produce a hash, it requires a long time and a lot of processing power. It therefore serves as proof that the miner who contributed the block to the blockchain worked hard to earn it. Each block carries the preceding block's unique hash, which serves as a link in the blockchain. The whole procedure is reflected in the following algorithm 1.

**Algorithm 1:** Verification of Proof Of Work and Hash value

```
previous_hash = self.last_block.compute_hash()
print("check hash ---------- {} :
  {}".format(previous_hash,block.previous_hash));
if (previous_hash ≠ block.previous_hash) then
    return False;
if self.is_valid_proof(block, proof) then
    print( "- - - - - - - - - - - -valid proof of
      work ____ ");
else
    return False;
end
block.hash = proof
self.chain.append(block);
return True
def is_valid_proof (self,block,block_hash)
        return (block_hash.startswith('0' *
  Blockchain.difficulty) and block_hash ==
  block.compute_hash())
def is_valid_proof (self,block)
        block.nonce = 0
        computed_hash=block.compute_hash();
        while not computed_hash.startswith('0' *
  Blockchain.difficulty) do
            block.nonce + = 1
            computed_hash=block.compute_hash();
            print(block);
end
return computed_hash,block
```

**Algorithm 2:** Creating and Adding new block to the blockchain

**input:** A set of N nodes in the current network, A block-chain B including blocks from $b_0$ to $b_n$, Consensus time $T_c$ required to create a new block.
**output:** A newly created block $b_{n+1}$
Initialize an empty set of transaction R = {};
$\beta \leftarrow WitnessElection(N)$;
**while** *transaction_time* $< t_c$ **do**
  **foreach** $n \in \mathcal{N} - \beta$ **do**
    $R \leftarrow R + GetTransactionsfromNode(n)$;
  **end**
**end**
$B_{n+1} \leftarrow createBlock(b_n, R)$;
**foreach** $n \in \mathcal{N} - \beta$ **do**
  signBlock($b_{n+1}, n$);
**end**
$B^{'} \leftarrow B + b_{n+1}$;
**foreach** $n \in \mathcal{N}$ **do**
  distributeBlockchain($B^{'}, n$);
**end**

TABLE I
MESSAGE BETWEEN TWO USERS WITH TIMESTAMP.

| User Name | Block | Message | Timestamp | Current Hash | Previous Hash |
|---|---|---|---|---|---|
| User (1) | Block-1 | Hello | 159724294956 | b249000da6a24160 4135868fc3160ed3 7e46e291b81a4b92 f97262f6ff26e26f1 | Null |
| User (2) | Block-1 | Hi Mahbub, How can I help you tonight? | 1597243145217 | 7ab9ff87049e3cc1 3309baf829732166 5ea85506019c0d49 c6fafa06c71b3b2f4 | b249000da6a24160 4135868fc3160ed3 7e46e291b81a4b92 f9762f6ff26e26f1 |
| User (1) | Block-2 | Does my Go Pro have a warranty? | 1597243237550 | 7b5de81284e0f518 4f196a591a89680f cfa0f6389e6df9dd 2c2814aaca957916 | 7ab9ff87049e3cc1 3309baf829732166 5ea85506019c0d49 c6fafa06c71b3b2f4 |
| User (2) | Block-2 | Can you tell me the serial number? | 1597243335447 | 01876c4359b4C950 58f6e38cfbb70e4 c38aec4b2a656cb9 dcC60c11982591ec9 | 7b5de81284e0f518 4f196a591a89680f cfa0f6389e6df9dd 2c2814aaca957916 |
| User (1) | Block-3 | Serial number is C769123567921389 | 1597243481445 | 7576257d3f2ea4a 39643b51eb3afab91 12f7656c91b093c92b 83c9e1331386f18b8 | 01876c4359b4C950 58f6e38cfbb70e4 c38aec4b2a656cb9 dcC60c11982591ec9 |
| User (2) | Block-3 | Thanks! It is still under warranty. | 1597243617259 | bc10d5a53a5952b 4215S5d5bfc197e 34f3af2b5bf91e4 7d8881bd21f26b0671 | 7576257d3f2ea4a3 9643b51eb3afab9112 f7656c91b093c92b 83c9e1331386f18b8 |
| User (1) | Block-4 | You are welcome. | 1597243728510 | 8b364aSffiff12 97b87922cle529b efb2Sce89b5446d5 3de1504cda5245ec223 | bc10d5a53a5952b 4215S5d5bfc197e 34f3af2b5bf91e47d 8881bd21f26b0671 |

The blockchain system is recommended by the majority of distributed consensus agreements. The PoW (Proof-Of-Work) agreement protocol is based on the response to a more complicated cryptographic picture, allowing orders to compete and finally return to the new degree of agreement. This technique of compliance is said to be extremely dependable, but it is connected with significant power consumption since it demands very high processing capacity from regions and, presently, an expensive dedicated hardware-based application for integrated circuits (ASIC). According to the PoS compliance protocol (Proof Of Stake), the new box's output should be supported, with an equal quantity for each stage kept on the network [23], [24], [27].

### *B. Block*

A block can be a group of transactions that are added to the blockchain [25], [26]. The block is made up of the miners, so the miner's job is to collect transactions from the group of transactions into a candidate block and add this candidate block for creating a blockchain. Our candidate block consists of a block header, which is essentially a bunch of metadata [28] [29] [30] about the block. We show how a new block is created and added in algorithm 2. Our block headers include the following required fields-Time-stamp, Message, Nonce, Sender, Receiver, Hash (a hash of the timestamp, index, data, and previous hash) Previous hash (the hash of the previous block).

*1) Time-stamp:* Timestamps are useful for keeping track of when data is shared, generated, or deleted on the internet. In certain instances, these archives are essential for us to comprehend the transaction mechanism as a whole. A timestamp, on the other hand, is more useful in certain situations. This is where 'trusted' time-stamping also comes into play [31] [32]. These timestamps are created by a reputable third party using stable federal information processing standards (FIPS) compliance hardware, so they can't be tampered with by a local customer. The client program [33] [34] receives the timestamp token and records it in the document or code signature [35].

*2) Nonce:* In the first block, we don't have block headers on our own. A nonce is an arbitrary number that is used only once in the cryptographic communication. Once a nonce is identified that works, the block is "resolved" and all the transactions in this block are added to the block-chain. The Genesis block is the one that performs the first transaction within the block that initiates the replacement electronic transaction [36].

*3) Hashing SHA-256:* We employed the SHA-256 hash algorithm in our system. The evidence of labor is made up of preset characters and numbers that correspond to the desired outcome. This is frequently represented using the SHA-256 hashing technique twice. This implies that once the goal hash is reached, the block is approved by the general public ledger based on the consensus of the other participating networks [37]. When the sender [38]–[41] sends a message, it goes to the server, and then the server stores this information and activates it to confirm and send the message to the receiver. In our messaging system, it can send 98% correct messages and detect fake messages effectively. We have shown the messaging structure of our block-chain based system in TABLE I. It is seen that our system generates a unique hash value each time a message is sent or received with a different timestamp. This proposed messaging framework provides a secured platform for messaging operations while enhancing security at the same time.

## V. CONCLUSION AND FUTURE WORKS

In blockchain, every block maintains the knowledge of the whole network as the block is attached to the chain, and it can be thought of as a finite database (a sequence of chains). Moreover, a blockchain is a static network that can be replicated across the whole shared network. The most

significant aspect of a blockchain-based system is that it does require any medium of trust authority. Instead, confidence is built by the mining process, which ensures the confidentiality and reliability of data applied to the system's chain of sites. That is why we have focused on blockchain-based peer-to-peer messaging systems for safety and reliability purposes. Using this blockchain-based shared network, messages can be interpreted, carried, tracked, and trusted without a doubt. This raises the message's consistency and protection. In our current system, only one-to-one communication has been implemented. And, it only supports text-based messages. We will improve these shortcomings in our further works in the future.

## REFERENCES


[1] K. Khacef, and G. Pujolle. "Secure Peer-to-Peer communication based on Blockchain." In Workshops of the International Conference on Advanced Information Networking and Applications, pp. 662-672. Springer, Cham, 2019.

[2] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam. "A new type of blockchain for secure message exchange in VANET." Digital communications and networks 6, no. 2 (2020): 177-186.

[3] F. Tschorsch, and B. Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys Tutorials 18, no. 3 (2016): 2084-2123.

[4] L. Shi, Z. Guo, and M. Xu. "Bitmessage Plus: A Blockchain-Based Communication Protocol With High Practicality." IEEE Access 9 (2021): 21618-21626.

[5] J. Han, Y. Yu, H. Lee, and J. Kang. "Current Status and Forecast of Blockchain Application in Security Technology." Advanced Multimedia and Ubiquitous Engineering (2021): 99-105.

[6] X. L. Liu, W. M. Wang, H. Guo, A. V. Barenji, Z. Li, and G. Q. Huang. "Industrial blockchain based framework for product lifecycle management in industry 4.0." Robotics and computer-integrated manufacturing 63 (2020): 101897.

[7] L. Arteiro, F. Lourenço, P. Escudeiro, and C. Ferreira. "Brain-Computer Interaction and Silent Speech Recognition on Decentralized Messaging Applications." In International Conference on Human-Computer Interaction, pp. 3-11. Springer, Cham, 2020.

[8] Biswas, Milon, et al. "Prototype Development of an Assistive Smart-Stick for the Visually Challenged Persons." 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). Vol. 2. IEEE, 2022.

[9] Y. Jiang, H. Bai, and H. Yang. "The Messaging Model Design Based Blockchain and Edge Computing for the Internet of Things." In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), pp. 604-608. IEEE, 2019.

[10] Biswas, Milon, et al. "Predicting Stock Market Price: A Logical Strategy using Deep Learning." 2021 IEEE 11th IEEE Symposium on Computer Applications Industrial Electronics (ISCAIE). IEEE, 2021.

[11] Biswas, Milon, et al. "BUVOTS: A Blockchain based Unmanipulated Voting Scheme." Rakib and Acharjee, Uzzal Kumar and Md, Whaiduzzaman, BUVOTS: A Blockchain Based Unmanipulated Voting Scheme (November 23, 2020) (2020).

[12] Biswas, Milon, and M. D. Whaiduzzaman. "Efficient mobile cloud computing through computation offloading." Int. J. Adv. Technol 10.2 (2018): 32.

[13] 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), vol. 1, pp. 317-322. IEEE, 2020.

[14] Song, G., Kim, S., Hwang, H., & Lee, K. (2019, January). Blockchain-based notarization for social media. In 2019 IEEE international conference on consumer electronics (icce) (pp. 1-2). IEEE.

[15] Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852.

[16] Biswas, Milon, et al. "BIoT: Blockchain based Smart Agriculture with Internet of Thing." 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). IEEE, 2021.

[17] Ahamed, Shahed, et al. "BPS: Blockchain Based Decentralized Secure and Versatile Light Payment System." Asian Journal of Research in Computer Science (2021): 12-20.

[18] Al-Amin, Sm, et al. "Towards a blockchain-based supply chain management for e-agro business system." Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Springer, Singapore, 2021.

[19] Datta, Papon, et al. "A secured smart national identity card management design using blockchain." 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT). IEEE, 2020.

[20] Mukherjee, Prodipta Promit, et al. "A Hyper-ledger Fabric Framework as a Service for Improved Quality E-voting System." 2020 IEEE Region 10 Symposium (TENSYMP). IEEE, 2020.

[21] Hossain, Md Parvez, et al. "Vehicle registration and information management using blockchain based distributed ledger from bangladesh perspective." 2020 IEEE Region 10 Symposium (TENSYMP). IEEE, 2020.

[22] Whaiduzzaman, Md, et al. "BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture." IEEE Access 9 (2021): 106655-106674.

[23] Biswas, Milon, et al. "Indoor Navigation Support System for Patients with Neurodegenerative Diseases." International Conference on Brain Informatics. Springer, Cham, 2021.

[24] Whaiduzzaman, M., Farjana, N., Barros, A., Mahi, M., Nayeen, J., Satu, M., Roy, S. and Fidge, C., 2021. HIBAF: A data security scheme for fog computing. Journal of High Speed Networks, (Preprint), pp.1-22.

[25] Akib, ASM Ahsanul Sarkar, et al. "Artificial intelligence humanoid bongo robot in bangladesh." 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). IEEE, 2019.

[26] Mahi, Md, et al. "A new unified communication approach to comply bandwidth optimization technique using dynamic channel allocation." International Journal of Computing and Network Technology 6.01 (2018): 1-11.

[27] Chaki, Sudipto, et al. "A Framework of an Obstacle Avoidance Robot for the Visually Impaired People." Proceedings of Trends in Electronics and Health Informatics. Springer, Singapore, 2022. 269-280.

[28] Mahi, Md, et al. "LCADP: a Low-Cost Accident Detection Prototype for a Vehicular Ad Hoc Network." Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering. Springer, Singapore, 2022.

[29] Biswas, Milon, and M. Shamim Kaiser. "DRLAS: Digital Record Keeping in Land Administration System Relying on Blockchain." Proceedings of Sixth International Congress on Information and Communication Technology. Springer, Singapore, 2022.

[30] Rahaman, Md Naimur, et al. "Lane Detection for Autonomous Vehicle Management: PHT Approach." 2021 24th International Conference on Computer and Information Technology (ICCIT). IEEE, 2021.

[31] Chaki, Sudipto, et al. "A Framework for LED Signboard Recognition for the Autonomous Vehicle Management System." 2021 International Conference on Science & Contemporary Technologies (ICSCT). IEEE, 2021.

[32] Ahmed, Shamim, Atanu Shome, and Milon Biswas. "DBST: A Scalable Peer-to-Peer Distributed Information System Supporting Multi-Attribute Range Query." 2021 International Conference on Science & Contemporary Technologies (ICSCT). IEEE, 2021.

[33] Jannat, Mifta Ul, et al. "Organic Food Supply Chain Traceability using Blockchain Technology." 2021 International Conference on Science & Contemporary Technologies (ICSCT). IEEE, 2021.

[34] Biswas, Milon, Jabed Al Faysal, and Kazi Asif Ahmed. "LandChain: A Blockchain Based Secured Land Registration System." 2021 International Conference on Science & Contemporary Technologies (ICSCT). IEEE, 2021.

[35] Gaur, Loveleen, Gurinder Singh, and Vernika Agarwal. "Leveraging artificial intelligence tools to combat the COVID-19 crisis." International Conference on Futuristic Trends in Networks and Computing Technologies. Springer, Singapore, 2020.

[36] Oberoi, Shelly, et al. "Determinants of Artificial Intelligence Systems and Its Impact on the Performance of Accounting Firms." Machine Learning, Advances in Computing, Renewable Energy and Communication. Springer, Singapore, 2022. 411-427.

[37] Gaur, Loveleen, et al. "Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels." Computers Electrical Engineering 95 (2021): 107374.

[38] Rana, Jyoti, et al. "Reinforcing customer journey through artificial intelligence: a review and research agenda." International Journal of Emerging Markets (2021).

[39] Ramakrishnan, Ravi, Loveleen Gaur, and Gurinder Singh. "Feasibility and Efficacy of BLE Beacon IoT Devices in Inventory Management at the Shop Floor." International Journal of Electrical Computer Engineering (2088-8708) 6.5 (2016).

[40] Afaq, Anam, and Loveleen Gaur. "The Rise of Robots to Help Combat Covid-19." 2021 International Conference on Technological Advancements and Innovations (ICTAI). IEEE, 2021.

[41] Gaur, Loveleen, et al. "Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels." Computers Electrical Engineering 95 (2021): 107374.