EMERGING ROLE OF BLOCKCHAIN TECHNOLOGY IN THE INTERNET OF THINGS

Md. Shakawat Hossain[1], Mani Manavalan[2*], Nur Mohammad Ali Chisty[3], Md. Mahofuzur Rahman[4]

[1]Department of Accounting & Information System, Jagannath University, Dhaka, Bangladesh
[2]Capgemini America, 79 5th Avenue, Suite 300, New York, NY 10003, United States
[3]Additional Superintendent of Police, Anti-Terrorism Unit, Bangladesh Police, Dhaka, Bangladesh
[4]Department of Business Administration, Port City International University, Bangladesh
[*]Corresponding Author: mani.manavalan@capgemini.com

ABSTRACT

The arising Blockchain innovation shows promising potential to improve modern frameworks and IoT via equipping various technologies and digital devices with additional data processing, handling, storage and its encryption. In the last decade, plenty of disrupting approaches and applications have arisen and considering that digital transformation and technical shift, a lot of blockchain technologies have put in a tremendous amount of effort and contribution from both modern and scholarly experts. With the introduction of this details survey of literature and existing papers, we have attempted to discuss the emerging role of technologies powered by blockchain innovation in enabling IoT frameworks. A blockchain-equipped IoT system is presented and essential methods are introduced. Also, major applications and key challenges are discussed as well. Thorough research for the latest ideas, patterns, and concerns is also discussed related to the Blockchain-enabled IoT.In this paper, an intensive survey on the most proficient approach to mold the technology of blockchain based on various requirements of IoT for enabling blockchain-based Internet of Things (BIoT) methodologies is introduced.After depicting the fundamentals, the most important applications are discussed to emphasize the effect of blockchain technology over traditional IoT applications. Then, the current challenges and potential improvements are discussed with regards to numerous perspectives that influence the design, advancement, and plan of BIoT applications. At last, a few ideas are identified determined to direct future BIoT experts and developers on a part of the issues that should be handled before deploying the next generation of BIoT applications.

Keywords: *Internet of Things (IoT), Blockchain Technology, Control Systems*

Introduction

Both Blockchain and the Internet of Things (IoT) are the two significant arising technologies of the traditional internet-empowered period of innovation. Both of these innovations are now at their pinnacle of influence while both are projected to almost require one more decade to totally develop. Indeed, comparing with early predictions, blockchain - without changing a lot - drifted at its present continuous pace on the development and hype. Unexpectedly, the IoT has advanced reasonably – winning inside a similar circular segment of the curve. Such relapse of IoT, as far as arriving at the development level, is somewhat justified by its far and wide reception in diverse applications and the security concerns raised to this point.

However, both of these technologies are distributed, independent, and decentralized frameworks having serious possibilities to support each other in the long run. IoT requires reinforcing its security while Blockchain has them because of its broad utilization of cryptographic systems and Blockchain needs contributions from the various nodes for its P2P (Peer-to-peer) model while IoT encapsulates them inside its engineering.

Blockchain innovation is a revolution in frameworks of record and has been anticipated by the business and research experts as an emerging tech that can have a huge part to play in checking, controlling, and, in particular, securing IoT gadgets (Panarello et al., 2018). The analysts depict a blueprint that work with the sharing of IoT resources and benefits and enable the automation of time-sensitive work processes cryptographically (Samaniego and Deters, 2016).

This paper discusses arrangements and workarounds to feature that the blockchain and IoT can be leveraged together. For instance, data communication by IoT gadgets is cryptographically proofed by the mark of the sender who holds a unique key pair; in this way, the validation and integrity of sent information are ensured. Besides, all exchanges

made to or by IoT gadgets are recorded on a distributed ledger that can be tracked easily. Although the blockchain may seem like an antidote to address the security layer of IoT that exists in centralized frameworks, there are still many challenges that hinder its integration into current IoT networks. As of late, there is an immense amount of speculation from the industries as well as huge interest from the academic world to carry out intense research with regards to these difficulties (Panchal et al., 2021; Raya et al., 2021; Ganapathy et al., 2021; Manojkumar et al., 2021; Sharma et al., 2021; Hussain et al., 2021). For instance, the risks related to the consensus protocols of blockchain technology are becoming a critical issue in the field. Besides, forks also carry threats to hinder the performance of consensus algorithms. Additionally, it has been observed that 51 percent of new blockchain technologies are prone to vulnerabilities (Bahack, 2013). Simultaneously, a lot of power has to be consume to support some of the high-end Blockchain (Ali et al., 2016).

Literature Review

Until a couple of years ago, blockchain innovation was just implemented with regards to payment systems, i.e., Bitcoin(Nakamoto, 2008) and Ether. Somewhat recently, increasingly more non-financial use cases for blockchain innovation emerged (Bynagari& Ahmed, 2021), for example, supply chain management and digital identification (Roeck et al., 2020). The later use cases identified the benefit of integrating blockchain with different innovations like IoT and AI.

For instance, Huh et al. (2017) examined the utilization of blockchain to further develop the framework foundation of different IoT gadgets. Dorri et al. (2017) defined how the engineering of blockchain can be changed to such an extent that the next framework is better prepared to equip IoT gadgets, particularly the speed of transactions. Other than focusing on a blockchain regarding IoT, a few papers also targeted the combination of blockchain and AI (Manavalan, 2020). Until this point, the emphasis is essentially on interfacing blockchain with another intelligent technology to make it savvier and faster, like IoT and AI, and not using all three technologies at the same time.

Nonetheless, the genuine capability of these new, arising innovations might be discovered only if these are combined. Singh et al. (2020) designed a blockchain-based framework that integrates IoT and AI. As opposed to Kumar Singh, this paper gives a non-specialized outline of the advantages of blockchain-based IoT applications and frameworks and how these two complement each other.

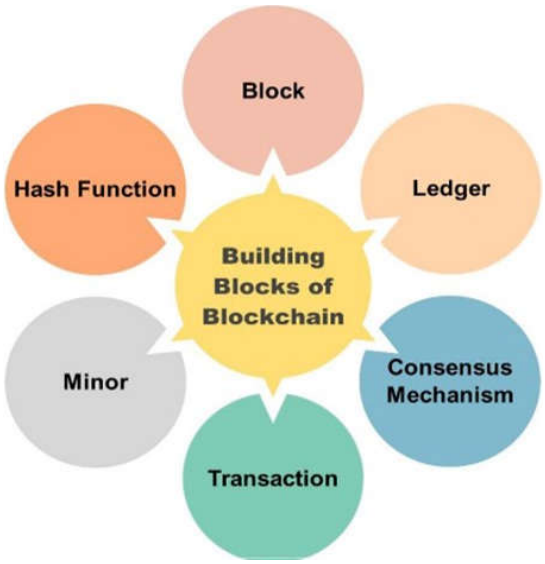

Fig. 1. Main Building Blocks of Blockchain Technology

Note that the ideas discussed in this paper apply to both public and private blockchain. The major difference between the two types of blockchain is that in a public blockchain each member can access the information stored on the blockchain. Whereas, in a private blockchain, access to information is limited to some specific parties. For the accomplishment of this paper, it is optional whether the access is public or private as the use cases could be executed on both blockchain types. Moreover, it should be noticed that blockchain, by some other database, is affected by poor data quality. Since this subject isn't related to blockchain-based data, it won't be talked about further in this paper.

Framework Of Decentralized Access Control Systems In IoT

The design presented in this section shows a decentralized framework where data with respect to access control is stored and handled

utilizing Blockchain.Each one of these participating entities are important for this framework other than IoT gadgets and the management hubs.

However, nodes in a network should incorporate a duplicate copy of the connected blockchain network. This infrastructure will be significantly huge and will continue to expand over timeBynagari, N. B. (2015); Fadziso, T., &Manavalan, M. (2017); Manavalan, M. (2014); Manavalan, M., &Bynagari, N. B. (2021); Neogy, T. K., &Bynagari, N. B. (2018). Most IoT gadgets cannot store blockchain data because of their nature. Thusly, our engineering does exclude IoT gadgets in the blockchain and, then again, characterizes another node that calls for access control data from the blockchain network for IoT devices.

Table 1: Simple comparison of IoT and Blockchain to different areas

Areas	**Internet of Things**	**Blockchain Technology**
Privacy	Lack of privacy and re-sources	Ensures that participating entities are secure
Bandwidth	Limited bandwidth and resources	High bandwidth
System Structure	Centralized	Decentralized
Scalability	Efficient to contain a large number of devices	Poor scalability with a large network
Resources	Restricted resources	Highly resource consuming
Latency	Low latency	Time-consuming
Security	Poor	Highly secure

Moreover, this framework includes a singular smart contract that characterizes each one of the activities allowed within the framework. The mentioned contract is unique and can't be erased from the framework. Components called 'managers' are required to communicate with the smart contract to characterize the access strategy of the overall framework.

Wireless Networks

A wireless network is a medium of communication within the network that allows correspondence in applications with restricted capacity and some prerequisites. Moreover, the IoT gadgets having a connection with the wireless network are somewhat restricted in their power, memory, and accessibility. IoT gadgets don't have a connection with the blockchain network here. Hence, one of the prerequisites of our engineering is that each one of the gadgets should be uniquely identified around the world in the network of blockchain technology. Whereas, public key generators can give a possible way out for the issue creating huge and complex values. Using the preexisting cryptographic methods would make a public key for each gadget. Therefore, authorizing encryption will make sure that all the identifiers in the framework are unique in nature.

Managers

In this framework, manager plays the role of a responsible entity who's answerable for dealing with the authorizations of IoT gadgets. Usually, these entities are considered as trivial nodes in the framework. Such nodes don't store any data or validate the transactions like the miner nodes do. Therefore, IoT gadgets can likewise play the role of managers in the framework. Furthermore, utilizing this methodology managers should be continually connected with the blockchain network, which assists with reducing the consumption of resources.In any case, enlisted IoT gadgets need to be assigned under a node of manager. This procedure is followed in order to keep managers away from enlisting gadgets under their nodes without approval from those devices. What's more, all enrolled IoT gadgets in the framework need to have a connection with at least one manager in the system. Otherwise, no one will be able to manage with that gadget. Nonetheless, an enlisted IoT gadget may have a connection with more than one manager simultaneously (Manavalan & Chisty, 2019).

Agent Nodes

This node within the decentralized network is an important element to deploy the main smart contract. Agent Node is the main proprietor of smart contract during the entirety of the

framework. When the smart contract is approved in the network, agent node is assigned an address that is directly connected to the smart contract. If communication has to be established within the network, each one of these nodes has to know the address of smart contract.

Smart Contract

The framework being discussed in this section is administered via the activities characterized in a smart contract. This is a unique agreement and can't be erased from the framework. Consequently, each one of the tasks allowed in the framework is characterized and is activated by the transactions carried out in blockchain.

When a transaction is activated through an exchange, the blockchain miners will store the data of that particular activity around the world. The activities and accessibility of smart contracts is likewise available all over the world. What's more, it should be understood that in this frameworks, only managers are the ones who can connect with smart contracts to characterize new strategies for the framework.

Blockchain Network

The blockchain entity in a framework is a private element to incorporate simplicity. In our case, a private blockchain is ideal because all of the components are diverse, ensuring a more solid result while assessing the framework. Be that as it may, in a real-world scenario, a public network of blockchain must be utilized to work with the mass adoption of the proposed solution.

On the other hand, private blockchain networks can be easily understood by anybody but just written by private nodes. These networks assist with keeping the whole blockchain secure and stable by keeping the record of exchanges and storing duplicates of the transactions. Various nodes can leverage the blockchain network to store and access the plan of action. This sort of data is completely decentralized and carefully designed.

Management Nodes

As referenced previously, IoT gadgets don't have a place with the blockchain network. Most IoT gadgets are extremely restrained. Those constraints confine IoT gadgets to be essential for such networks. Being essential for the network refers to keeping a complete tracking data of blockchain transactions and creating duplicates of them locally.

These nodes, often referred to as 'management nodes', are integrated directly with a node of blockchain itself. Various networks can be interfaced with a management node and we can also connect various other nodes with the same blockchain node. IoT gadgets may have the option to demand access data from the network using these nodes.

Why Blockchain For Iot? – Determining The Need For Blockchain

Before diving into the details on the best way to utilize a blockchain for IoT applications, it should be first determined that a blockchain isn't generally the best answer for each IoT situation. Customary databases or DAG (Directed Acyclic Chart) ledgers might be a superior fit for certain IoT applications. In particular, to decide whether the utilization of a blockchain is fitting, an engineer must choose if the following features are fundamental for an IoT application.

Table 2: Brief comparison of public, private, and consortium Blockchain

	Public Blockchain	**Private Blockchain**	**Consortium Blockchain**
Participation in Consensus	All nodes	Single network	Selected nodes in multiple networks
Access	Public read/write	Can be limited	Can be limited
Identity	Pseudo-anonymous	Approved entities	Approved entities
Immutability	Yes	Partial	Partial
Transaction Processing Speed	Slow	Fast	Fast
Permission-less	Yes	No	No

Decentralization

IoT applications request decentralization when there isn't any reliable framework. Be that as it may, numerous users blindly trust certain organizations, government offices, or banks, so

in case there is common trust, a blockchain isn't needed.

P2P Transactions

In IoT, most of the communication goes from nodes to gateways that direct the information to a remote server or cloud. Interchanges among peers at a node level are really not normal, aside from some specific applications. Some additionally different ideal models cultivate communication among nodes at a similar level, as it occurs in fog computing with local routes.

Decentralized Payment Systems

Some IoT applications might need to perform financial exchanges with third parties, and some applications don't. Also, financial exchanges can be carried out by traditional payment frameworks, despite the fact that they typically infer to pay transaction costs and it is important to trust banks or any middle man.

Public Sequential Transaction Logging

Numerous IoT networks collect information that should be time-stamped and stored consecutively. In any case, such requirements might be handily satisfied with conventional databases, particularly in situations where security is ensured or where cyber threats are uncommon.

Distributed Systems

Distributed frameworks can likewise be based on top of cloud servers or any type of traditionally distributed framework. The need for this element isn't sufficient to justify the utilization of a blockchain. There also must be an absence of trust in the content that deals with the distributed computing framework.

Collection of Micro-transactions

Some IoT applications might have to track each transaction to keep up with visibility, for accountability purposes or because that big data methods will be applied afterward. In these circumstances, a blockchain might be helpful. Be that as it may, different applications don't have to store each collected value.For instance, in remote agricultural tracking, where communication is pretty much costly, it is common to utilize IoT hubs that come into play consistently to acquire information from sensors. In such cases, a local framework might collect and store the information, and when daily it sends the collected data all together in one transaction.

Major Applications Of Blockchain Technology For Iot

IoT in Healthcare

The utilization of Internet of Things in medical care has enabled field experts to manage the healthcare systems with medical information identified with the patients, their families, their close ones, and also the medical care experts. Healthcare information called such as EMR (Electronic Medical Records) is stored by medical experts due to its sensitive nature. To work with healthcare data, there are more advanced mechanics such as EHRs (Electronic Health Records) having a more detailed information structure as compared to the former.To facilitate the possibility of the distributed databases, a new methodology based on a blockchain approach has been introduced lately. In this model of blockchain, a block is initiated and shared when new data related to patients and their medical records is recorded. In this way, we have an improved sense of data accessibility and portability about patients.

IoT in 5G

In the generation where IoT is taking higher and higher leaps, 5G will empower a completely portable and interconnected environment for millions of digital objects and devices. To effectively address and solve the issues related to privacy and protection of data in the 5G-enabled ecosystem, a security framework supported by blockchain and data sharing plan would come in handy.This approach shall be based on the idea of adding different building blocks to the network of blockchain where each new block is integrated with the network through its hash value. It's noteworthy that the past value can be perceived from the block header easily.

IoT in Vehicles

The idea of incorporating IoT in vehicles is emerging. It enables the addition of vehicle systems into the new generation of IoT to build up intelligent correspondence among vehicles and connected networks. Nonetheless, some

new papers attempt to carry out a blockchain approach to IoV. Firmly based on a decentralized model, Huang et al. presented a model for EVs and their management of charging activities. The model uses ECC, generally known as Elliptic Curve Cryptography, to compute values of electric vehicles and stations where EVs are charged.

Collaborative Video Delivery

Delivery of excellent graphical content in the IoT these days is a challenge to tackle for internet service providers. To cope up with that, experts proposed a processing tool for collaborative video delivery based on absolutely decentralized technology. In particular, this service is based on 3 blockchains specifically as follows: the content facilitating blockchain, the delivery checking blockchain, and the monitoring blockchain.

IoT in Cloud

Billions of IoT gadgets transfer their information using cloud platforms. Experts presented a smart resource management tool for remote servers based on blockchain innovation, in order to eliminate the heavy costs resulting due to power consumption. In this model, users use their private keys to label a transaction carried out through blockchain-based exchanges, while the local users look for the transmission transactions. In the end, whole block is disposed of if it doesn't go through the validation step.

Challenges In Integrating Blockchain With Iot

Adding blockchain to IoT poses further functional and technical challenges since the advancement of BIoT applications is a complicated process that is influenced by numerous perspectives that are interrelated. The primary challenges are depicted in the following subsections.

Data Privacy

Each one of the users of a blockchain is recognized by its public key or its hash. This implies that secrecy isn't ensured and, since all exchanges are shared, it is feasible for outsiders to analyze such exchanges and collect the actual identifications of the members. Data privacy is considerably more complicated in IoT conditions since IoT gadgets can reveal private client information that could be stored in a blockchain whose security prerequisites vary starting with one country then onto the next (Bynagari& Amin, 2019; Manavalan, 2018).

Identity verification may likewise be an issue in IoT: if an entity is answerable for approving users, it can likewise have the option to block them. To address such a challenge, it is proposed that a permissioned blockchain must be used for accessing and dealing with numerous IoT nodes. The proposed framework gives an overall entity verification management that increases security and privacy against cyber-attacks by randomizing keys. Such keys are produced locally on the gadget and they are never shared from it.

Scalability and Storage Issues

Data limit and issues related to scaling huge amount of data have been profoundly addressed in the literature. In this tech, the network is continually progressing, at a pace of one megabyte per block within every ten minutes, and duplicates have been stored along with the blockchain nodes (Manavalan&Ganapathy, 2014). However only some specific full nodes store the complete data where data storage needs are critical.

As the size of the data block develops, nodes require an ever-increasing number of storage resources, in this manner lessening the framework's ability to scale. What's more, a large chain affects the execution of the framework, for example, it increases synchronization time for new users.

Energy Efficiency

Usually, IoT nodes use resourceful hardware that is fueled by batteries. Along these lines, energy efficiency is vital to empower a dependable node arrangement. However, numerous blockchains are shown to be huge consumers of power. In such cases the greater part of this huge energy consumption is because of two elements:

- **Mining:**Blockchains like Bitcoin use huge amounts of power because of the mining system, which includes a consensus protocol that comprises brute force to locate a hash.

- **P2P interchanges:** P2P interchanges require edge gadgets that must be controlled, which could prompt the waste of energy. A few experts proposed energy-effective conventions for P2P networks, however, the issue actually must be read further for the particular instance of IoT networks.

Conclusion

The standard of the Internet of Things (IoT) is structuring the pathway for a digitally modern world, where a large number of our everyday objects will be interconnected and will connect within an ecosystem to collect relevant data and automate certain tasks. Such an accomplishment needs, in addition to other things, consistent validation, data protection, security, right strategies against cyber-attacks, easy deployment of frameworks, and regular maintenance. Such provisions can be brought by blockchain, an innovation brought into the world with a digital currency called Bitcoin. Within an ecosystem of complicated IoT devices and applications, different gadgets are interconnected to develop, gather, scale, deploy, and store information. The enterprises are showing strong curiosity in promoting the combination of both IoT and blockchain-supported business work processes.Because of these fast achievement in these fields and ideas on plans of action, IoT is relied upon to be highly applicable in multiple ventures.

Through this paper, we have gained insights regarding the possible mixture of IoT and blockchain technology from a new perspective. An IoT system completely backed by decentralized capacity of blockchain has been presented and relevant applications are discussed. We've also tried to shed some light on the challenges that are faced by field experts more often than not. Along with these challenges and difficulties, we have presented the hindrances identified with research patterns related to blockchain-empowered IoT.

With a few difficulties introduced in IoT engineering, integrating the IoT into one of the distributed technologies might be the right decision. Among the normal types of distributed technologies is the blockchain. It uses a decentralized methodology that conveys better productivity and reduces the occurrence of a weak point.The integration of blockchain with IoT can resolve issues of the IoT frameworks and provide an effective method for future works. Hence, the purpose of this paper was to give a thorough idea of coordinating the IoT frameworks with blockchain innovation. After introducing the basis of IoT and blockchain, the paper gave an extensive insight into how blockchain presents better use cases for IoT applications in various fields.

Moreover, ongoing research introducing the combination of IoT and blockchain is likewise introduced. Then, blockchain as a service for the IoT is looked upon to show how different provisions of blockchain can be implemented for different IoT sectors.

References

1. Ali, M., Nelson, J., Shea, R., and Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains. In Proc. Annual Technical Conference (USENIX ATC), pp. 181–194.
2. Bahack, L. (2013). Theoretical Bitcoin attacks with less than half of the computational power. Cryptography and Security, 1-18. https://arxiv.org/abs /1312.7013
3. Bynagari, N. B. & Ahmed, A. A. A. (2021). Anti-Money Laundering Recognition through the Gradient Boosting Classifier. Academy of Accounting and Financial Studies Journal, 25(5), 1–11. https://doi.org/10.5281/ zenodo.5523918
4. Bynagari, N. B. (2015). Machine Learning and Artificial Intelligence in Online Fake Transaction Alerting. Engineering International, 3(2), 115-126. https://doi.org/10.18034/ei.v3i2.566
5. Bynagari, N. B., & Amin, R. (2019). Information Acquisition Driven by Reinforcement in Non-Deterministic Environments. American Journal of Trade and Policy, 6(3), 107-112. https://doi.org/10.18034/ajtp.v6i3.569

6. Dorri, A., Kanhere, S., and Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. In Proceedings of the IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation
7. Fadziso, T., &Manavalan, M. (2017). Identical by Descent (IBD): Investigation of the Genetic Ties between Africans, Denisovans, and Neandertals. Asian Journal of Humanity, Art and Literature, 4(2), 157-170. https://doi.org/10.18034/ajhal.v4i2.582
8. Ganapathy, A., Vadlamudi, S., Ahmed, A. A. A., Hossain, M. S., Islam, M. A. (2021). HTML Content and Cascading Tree Sheets: Overview of Improving Web Content Visualization. Turkish Online Journal of Qualitative Inquiry, 12(3), 2428-2438. https://doi.org/10.5281/zenodo.5522159
9. Huh, S., Cho, S., and Kim, S. (2017). Managing IoT devices using a blockchain platform. In Proceedings of the 19th International Conference on Advanced Communication Technology (Piscataway, NJ: IEEE), 464–467.
10. Hussain, S., Ahmed, A. A. A., Kurniullah, A. Z., Ramirez-Asis, E., Al-Awawdeh, N., Al-Shamayleh, N. J. M., Julca-Guerrero, F. (2021). Protection against Letters of Credit Fraud. Journal of Legal, Ethical and Regulatory Issues, 24(Special Issue 1), 1-11. https://doi.org/10.5281/zenodo.5507840
11. Manavalan, M. (2014). Fast Model-based Protein Homology Discovery without Alignment. Asia Pacific Journal of Energy and Environment, 1(2), 169-184. https://doi.org/10.18034/apjee.v1i2.580
12. Manavalan, M. (2018). Do Internals of Neural Networks Make Sense in the Context of Hydrology? . Asian Journal of Applied Science and Engineering, 7, 75–84. Retrieved from https://upright.pub/index.php/ajase/article/view/41
13. Manavalan, M. (2020). Diagnosing Epidermal basal Squamous Cell Carcinoma in High-resolution, and Poorly Labeled Histopathological Imaging. Engineering International, 8(2), 139-148. https://doi.org/10.18034/ei.v8i2.574
14. Manavalan, M., &Bynagari, N. B. (2021). Repurposing High-Throughput Imaging Tests for Drug Discovery Allows for Biological Activity Prediction. International Journal of Aquatic Science, 12(3), 2431-2443.
15. Manavalan, M., & Chisty, N. M. A. (2019). Visualizing the Impact of Cyberattacks on Web-Based Transactions on Large-Scale Data and Knowledge Based Systems. Engineering International, 7(2), 95-104. https://doi.org/10.18034/ei.v7i2.578
16. Manavalan, M., &Ganapathy, A. (2014). Reinforcement Learning in Robotics. Engineering International, 2(2), 113-124. https://doi.org/10.18034/ei.v2i2.572
17. Manojkumar, P., Suresh, M., Ahmed, A. A. A., Panchal, H., Rajan, C. C. A., Dheepanchakkravarthy, A., Geetha, A., Gunapriya, B., Mann, S., &Sadasivuni, K. K. (2021). A novel home automation distributed server management system using Internet of Things. International Journal of Ambient Energy,https://doi.org/10.1080/01430750.2021.1953590
18. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available online at: https://git.dhimmel.com/bitcoin-whitepaper/
19. Neogy, T. K., &Bynagari, N. B. (2018). Gradient Descent is a Technique for Learning to Learn. Asian Journal of Humanity, Art and Literature, 5(2), 145-156. https://doi.org/10.18034/ajhal.v5i2.578
20. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. Sensors, 18, 2575.
21. Panchal, H., Sadasivuni, K. K., Ahmed, A. A. A., Hishan, S. S., Doranehgard, M. H., Essa, F. A., Shanmugan, S., & Khalid, M. (2021). Graphite powder mixed with black paint on the absorber plate of the solar still to enhance yield: An experimental investigation. Desalination, Volume 520. https://doi.org/10.1016/j.desal.2021.115349
22. Raya, I., Kzar, H. H., Mahmoud, Z. H., Ahmed, A. A. A., Ibatova, A. Z., &Kianfar, E. (2021). A review of gas

sensors based on carbon nanomaterial. Carbon Letters. Article No: 276. https://doi.org/10.1007/s42823-021-00276-9

23. Roeck, D., Schoneseiffen, F., Greger, M., and Hofmann, E. (2020). Analyzing the potential of DLT-based applications in smart factories. In Blockchain and Distributed Ledger Technology Use Cases - Applications and Lessons Learned, eds H. Treiblmaier and T. Clohessy (Cham: Springer), 245–266.
24. Samaniego, M., and Deters, R. (2016). Blockchain as a Service for IoT. In Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016.
25. Sharma, D. K., Chakravarthi, D. S., Shaikh, A. A., Ahmed, A. A. A., Jaiswal, S., Naved, M. (2021). The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique. Materials Today: Proceedings.https://doi.org/10.1016/j.matpr.2021.07.388
26. Singh, S. K., Rathore, S., Park, J. H. (2020). BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Generation Computer Systems, Volume 110, 721-743. https://doi.org/10.1016/j.future.2019.09.002