**J**ournal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, No. 1, (2022),
ISSN : **1906-9685**


# ENHANCED SECURITY: THE PERSPECTIVE OF INTEGRATING BLOCKCHAIN AND IOT

**[#1]KISHOR KUMAR GAJULA,** ***Assistant Professor,*** **Department of Computer Science and Engineering,**

**[#2]Dr.Y. VENKATESHWARLU,** ***Professor,*** **Department of Computer Science and Engineering**

**MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.**

**ABSTRACT:** Blockchain, a Bitcoin offshoot, has received a lot of attention for the potential it shows in other areas, particularly in very complex non-financial systems. A Blockchain-powered distributed ledger can achieve a high level of security and immutability by combining cryptographic methods like hashing and asymmetric encryption with a distributed consensus mechanism. The requirement for go-betweens is therefore eliminated. On the other side, there are too many Internet of Things (IoT) gadgets connected to the network. This occurrence represents a more serious threat to confidentiality and safety. As a result, it is essential to address the security issues that have emerged in the expanding IoT ecosystem. This research looks into how blockchain could be used to make the Internet of Things safer and more private. For this assessment, we looked at how Blockchain (BC) has been used for IoT security in recent academic papers and projects/applications. The goal was to determine what was standing in the way of using BC to make the IoT ecosystem safer, and then to suggest ways to overcome those difficulties.

***Keywords:*** *Blockchain, Distributed Ledger Technology (DLT), Internet of Things (IoT), Proof-of-Work (PoW), Security.*

## 1. INTRODUCTION

In this article, we take a look at how Blockchain of Things (BCoT) could become more widespread and how Blockchain technology could be used to bolster the safety of Internet of Things networks. Despite the revolutionary nature of blockchain, this article focuses on research from the previous decade. This research looks into how Blockchain could be used to strengthen the safety of IoT devices and networks. In order to accomplish this goal, researchers are examining blockchain and related digital ledger technologies to learn more about their potential uses, restrictions, privacy and security issues. The 2018 International Conference on Emerging Technologies in Computing was held at London Metropolitan University, and this publication provides a succinct review of the results obtained there. The IoT ecosystem promotes security and privacy just like traditional IT companies. Since blockchain fortifies the very foundation of the IoT, it is widely recognized as indispensable for protecting users' personal data and security. Blockchain experts and researchers are always looking for new applications and perspectives. To solve complex mathematical problems, computers use a technique called proof-of-work (PoW). A

central digital database that logs all transactions safeguards the blockchain's veracity. The deals have been sealed. In Figure 1, we see a high-level, simplified system block diagram of BC technology in action. The effects of social media on psychological health are investigated.

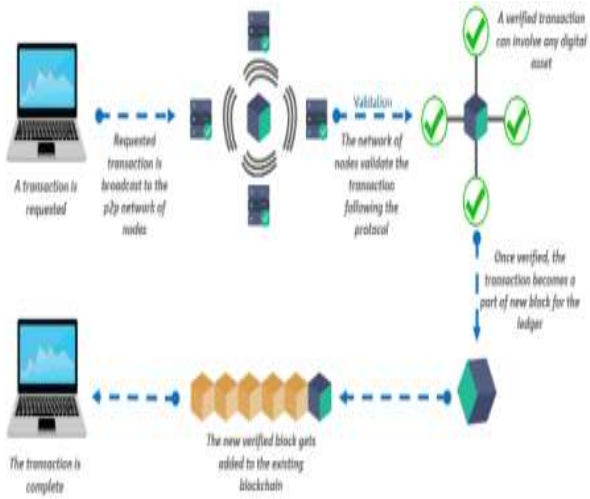


**Figure1.**Blockchain concept overview.

The highest possible level of safety during user ID registration is ensured by the Blockchain technology's Public Key, which is deliberately unpredictable. This ensures a higher level of privacy. Blockchain technology's applicability outside of the financial sector has been acknowledged in a number of research papers and project summaries. Human resource management, cloud storage, electronic voting, location verification, distributed cloud computing, securities settlement, and recruitment are all examples of such systems. The diagram depicts the six-tiered hierarchy of a blockchain system. We'll get into the second, labeled "2," point in the next paragraph.

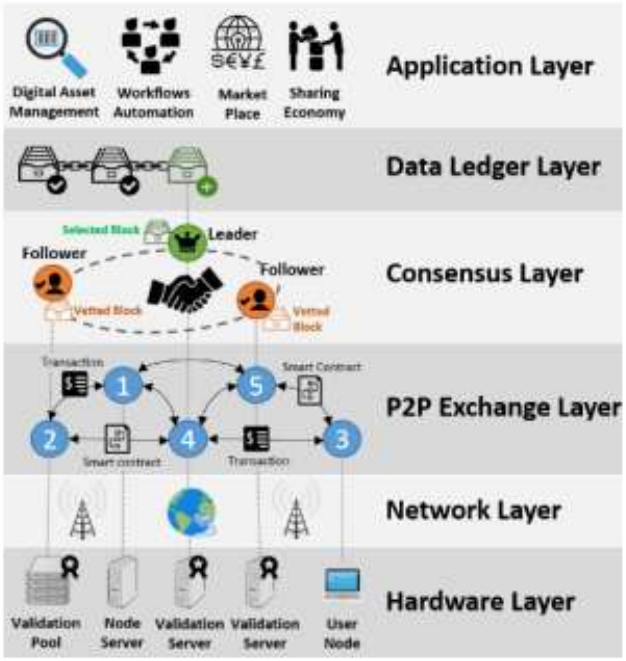


**Figure2.**Blockchain Technology Layer Model

Blockchain Technology's Layered Architecture

The purpose of this research was to determine whether or not Blockchain technology has the ability to improve the security of Internet of Things (IoT) systems by analyzing the scholarly literature and relevant projects/applications. In addition, they highlighted the difficulties of implementing Blockchain in this area and suggested improvements to Blockchain-based IoT security solutions. Examines the areas of expertise surrounding Blockchain and digital currencies, including the Internet of Things, the Internet of Everything, Wireless Sensor Networks, and Distributed Ledger Technology (DLT).

## 2.BLOCKCHAINFUNDAMENTALS

To truly grasp Blockchain's potential for boosting the security of the IoT, one must get a deep familiarity with its inner workings. The next session will delve into the complexities of the IoT ecosystem after this brief introduction to Blockchain.

There are two nodes and an intermediary in a blockchain. The goods consist of the following:

**Transaction:** In blockchain-like digital ledgers, participants start transactions.

**Block:**

Blocks on a blockchain not only record

transactions, but also incorporate meta-data like timestamps and the order in which they were generated.

Depending on their use, blockchains can be labeled as either public or private. Most public blockchains can be viewed and altered by anybody. Every Bitcoin transaction is publicly and easily viewable on the Blockchain. Depending on their use, public Blockchains may restrict both read and write access. Users' anonymity is protected on a private Blockchain network. Only trusted members or a single company have access. "Consortium blockchain" technology is being mandated by government bodies and their subsidiaries. Because it is available to the public, this technology is both secure and convenient. Each node in a distributed network has its own blockchain, which is constantly refreshed with new data records and transactions to ensure the reliability of the distributed ledger. The public has the ability to verify any unauthorized or accidental changes. To maintain security and privacy, the public blocks are hashed and encrypted with a private key. Inaccessible information is that which has been encrypted with the private key.

Blockchain can be used centrally, but its decentralized nature is its defining characteristic. These causes contribute to its decentralized nature:

Multiple nodes, as opposed to a single node, are responsible for recording transactions and blocks in a blockchain network.

The authority of a single body is diminished when rules or algorithms are used to validate transactions. Gaining consensus on this strategy calls for a lot of certainty.

In order for a transaction to be included in a blockchain, it must first be confirmed. Previous links between blocks are immutable because they are transparent and may be independently verified. When compared to other technologies, blockchain ecosystems fall short on the security front. The blockchain does not immediately reflect new transactions. Nodes make up the blockchain network. A transaction must be confirmed and verified before it can be added to the chain. Nodes in a blockchain network must adhere to a set of rules or algorithms in order for the network to function properly. Data authenticity on a Blockchain is determined using a set of criteria established by many algorithms. Numerous transactions can be found in a single block. The new block is broadcast throughout the Blockchain network, where each node can then choose to add it to its own blockchain. Each next block in the chain incorporates the hash or digital footprint of the prior block.


**Figure3.**A typical blockchain implementation

New transactions are verified by the Blockchain, and their records are stored in perpetuity. There is also a guarantee of the user's or participant's anonymity. Information provided by the user during the verification procedure is kept secure. To facilitate thorough cooperation, all dealings are recorded in a digital ledger accessible via computer. Instead of depending on trust or a third party to settle disputes, blockchain participants put their faith in the system's decentralized design. For those unfamiliar, "Blockchain" is shorthand for "Trust Machine."

Bitcoin was an early adopter of the decentralized ledger system known as the Blockchain. Healthcare, HR, recruitment, legal document management and validation (including deeds and certificates), IoT, the cloud, and other areas can all benefit from blockchain technology. According to Tapscott (year), blockchain is best understood as a "World Wide Ledger" that may be put to creative use beyond just recording financial

transactions. Independent government services, accumulated knowledge, and decentralized communities are all good examples. Just how much. The essay delves into the conventional and cutting-edge uses of blockchain technology. Blockchain technology is shown in action in Figure 1. The multiple applications in biology are depicted in the fourth picture. Just how much. Access control, non-repudiation, data versioning, integrity, auditing, and provenance are six further reasons listed in the paper for using blockchain technology.

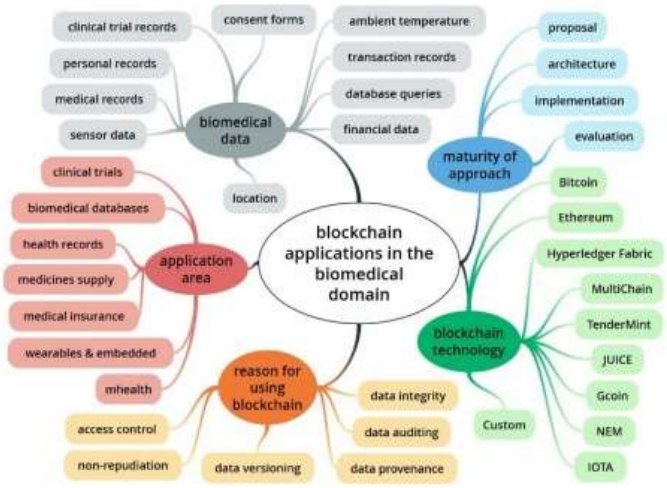


**Figure4.**Blockchain visualization in biomedicine.

## 3. INTERNET OF THINGS (IOT)

The term "Internet of Things" (sometimes "Internet of Objects") is used to describe the networked electronic and electrical devices of any size or function. With the exception of the Internet, the majority of this connection consists of wireless sensors. Because of the explosion of IoT gadgets, communication is no longer limited to exchanges between machines. An extensive variety of protocols, software, and networks are all within the capabilities of IoT gadgets. Sensor networks, radio frequency identification, ZigBee, and location-based technologies are just some of the ways that the Internet of Things is being propelled.

As more inanimate objects become Internet-connected without human mediators, Internet Business Solutions Group (IBSG) labeled this phenomenon "the Internet of Things" (IoT). Significant increases in velocity have been observed across a wide range of domains, from CISCO's 'Planetary Skin' to the Smart Grid and intelligent vehicle IoT. Consumers will be more likely to utilize the Internet if more devices are built into their everyday appliances, particularly those that are kept close to their bodies. Internet of Things (IoT) gadgets don't have any peer-to-peer or Internet-facing interfaces, but they do use Internet networking protocols. This limitation calls for immediate response.

The Internet of Things (IoT) can improve privacy, security, and administration through the integration of automobile electronics, home environmental management systems, telephone networks, and domestic utility service control mechanisms. It's clear that IoT and network connectivity are spreading rapidly. The five main parts of an IoT ecosystem are:

**Sensors**: Data collecting and conversion require sensors.

**Computing Node**: Processing sensor data requires CPU-powered nodes.

**Receiver**: A transceiver is a device that can receive signals from other devices, including both close and faraway computer nodes.

**Actuator**: The Computing Node can make a decision regarding which electromechanical actuator to use. The Internet-connected device reboots after processing data from its sensors and the web.

**Device**: It executes a task when activated.

## 4. BC ENABLED ENHANCED IOT SECURITY

In an Internet of Things (IoT) setting, machine-to-machine (M2M) communication predominates. The issue of machine trust has not been adequately addressed by the Internet of Things (IoT). Improved scalability, security, reliability, and anonymity are just some of the benefits of blockchain technology. Blockchain can manage and coordinate the execution of transactions across a wide variety of Internet of Things gadgets. In fact, "Shodan," the first search engine made for Internet-connected devices, will identify vulnerable IoT gadgets and draw attention to the

need for fixing them. The introduction of blockchain technology into IoT ecosystems removes all points of failure and greatly increases the system's reliability. Encryption using cryptography and hashing to protect sensitive information. The use of blockchain technology may improve the safety of Internet of Things gadgets. Unfortunately, neither hashing nor cryptographic processes are within the capabilities of IoT devices. This limitation necessitates more study aimed at increasing the useful life of the existing power source. According to Underwood, Blockchain has the potential to completely alter the e-commerce industry. Blockchain was designed to guarantee honesty above everything else. Blockchain is a robust network system that can reliably collect and sequentially store transaction data. Private securities transactions on the NASDAQ are reliably recorded thanks to the 'Linq blockchain' system. Specifically for swaps, Axoni and DTCC offer post-trade financial solutions. Prioritize regulatory initiatives like British Columbia's secure, trustworthy, and easily accessible real-time monitoring system for financial transactions. Using blockchain technology, the risks connected with data manipulation and dishonesty can be reduced while industrial IoT and OT equipment is monitored and protected in real time. Once the blockchain is up and running, it can be used to prevent tampering by securely storing data about compromised sensors, devices, and controllers.

Internet of Things (IoT) devices' privacy and security are compromised by Wireless Sensor Network (WSN) technologies. Due to its robust design, consensus mechanism, and use of cryptographic technologies, Blockchain has been labeled a Trust Machine. Risks to security in the Internet of Things (IoT) can be reduced in many instances. Miraz speculates that blockchain technology and the Internet of Things (IoT) might coexist. Consensus in BC relies on a network of active nodes, and the IoT can help make that happen. The security of IoT gadgets can be bolstered with the help of blockchain technology. Transparency, privacy, immutability, and operational sturdiness are all characteristics used as examples.

When physical and digital systems are interconnected, as they are in the IoT, a networked world is born. There have been a number of obstacles that have slowed the full incorporation of IoT security into device and product design. Internet of Things (IoT) study has been revolutionized by the application of blockchain technology. By bringing together IoT and BC, we can increase system resilience, make it easier to recover from cyber threats, and strengthen overall security. However, the slow development of these technologies creates a number of challenges for their implementation. Research overwhelmingly favors using blockchain to protect IoT networks against "Stalker" attacks and other vulnerabilities.

For the Internet of Things to work, wireless sensor networks must be implemented. DDoS assaults can affect any gadget connected to the internet because of their inherent lack of security. If any of these nodes are compromised, the network as a whole is at risk. Cloud computing is essential to the functioning of IoT networks. The existence of SPF makes centralized architecture more susceptible to attack.

Data from IoT devices is transmitted in bulk for real-time analysis and decision making. The safety of sensitive information and the authentication of users are crucial components of the Internet of Things. In the absence of safeguards, massive data collection can be abused. Therefore, protecting the IoT system from injection attacks and spoofing is crucial. By inserting erroneous or misleading data or measurements, injection attacks alter the system's decision-making.

Sensors that provide data can share it with other autonomous systems and marketplaces in the Machine Economy. However, trust building among stakeholders remains a major challenge. The problem of non-repudiation can be solved without resorting to a third party if a method is implemented that permits public verification of an audit trail. FileCoins and Trans Active Grids are two examples of legitimate use cases for blockchain technology. These applications allow

devices to trade products and services with one another, increasing the potential for monetary benefit.

Pseudonymization occurs before personal information is sent to Internet-connected smart home appliances. Using cryptographic hashes, the blockchain checks and validates information from IoT devices. In order to reconstruct data and establish access protocols for smart devices and service providers, the owner makes use of public keys. Layers of the BC structure are shown in Figure 1. The digit 2. Address vulnerabilities in software, data, communication, and the physical environment. Ethereum's smart contracts use blockchain technology, which functions as a distributed ledger. The BC (Blockchain) application layer prevents unauthorized interference with dependent operations.

Bahga and Madisetti came up with a novel strategy to combine Cloud-Based Manufacturing (CBM) and Business Process Integration of Internet of Things (BPIIoT). With this method, you can access a cloud service that provides access to manufacturing resources and abilities. Using smart contracts and regenerating public keys, the safety of Ethereum transactions was ensured. Korpela et al. investigate how cloud computing, the Internet of Things, and blockchain (BC) can meet the unique integration requirements of supply chains. Low-cost supply chain management options are available through cloud computing and the Internet of Things. Blockchain technology may drastically alter today's digital supply chains. Smart energy could be traded via Internet of Things (IoT) devices, made possible by blockchain technology, as part of the rollout of Industry 4.0. This is crucial since blockchain was designed for interactions between autonomous computers. Smart devices can now allow the selling of steam and natural gas thanks to blockchain technology. Through blockchain transactions, energy producers make their prices public, while customers use bitcoin to shop around for the best deal.

The group's open-source cryptocurrency, IOTA, facilitates micropayments across the IoT. The TANGLE protocol is the breakthrough blockchain technology developed by IOTA. Because of its acyclic network design, TANGLE is more scalable than block-and-miner blockchains.

Incorporating both level 0 and level N protections, the Internet of Things security framework created by Chakraborty et al. This framework keeps nodes with few resources running smoothly. Primitives under level 0 security can only do so much computation. Primary and secondary nodes can be found on level N. Data processing, communication, and security are all primary functions provided by nodes. On the flip side, secondary nodes are there to prop up primary ones. Due to lack of resources, level 0 nodes are unable to make direct connections with other nodes. The N-level nodes can make private third-party connections.

## 5. CONCLUSION

The use of blockchain technology enhances safety measures. This article discusses the methods used by two emerging technologies—IoT ecosystems and AI—to carry out their functions. Internet of Things security is also discussed. Additionally, Blockchain's potential for protecting IoT environments is investigated.

Blockchain and the Internet of Things hold great potential in many different fields. In addition to its role in the creation and exchange of bitcoins, blockchain has also proven useful in guaranteeing the safety of financial transactions over computer networks. The IoT is expanding beyond its initial application of wireless sensor networks. Blockchain outperforms earlier technology in areas including privacy, security, traceability, data provenance, and time stamping. Human-to-human (H2H), machine-to-machine (M2M), and machine-to-human (H2M) transactions are all protected. With the proliferation of IoT devices, blockchain technology has proven to be exceptionally trustworthy. This distributed solution supports the continued viability of Internet design by providing for data redundancy via geographically dispersed storage.

**REFERENCES**


1. Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security", Proc. of the Int.Conf.onEmergingTechnologiesinComputing2018(iCETiC'18),PartoftheLectureNotesoftheInstituteforComputerSciences,SocialInformaticsandTelecommunicationsEngineering(LNICST),vol.200,London,UK,2018,pp.38-46.Available:https://link.springer.com/chapter/10.1007/978-3-319-95450-9_3.
2. Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Safeeullah Soomro, Mohammad Riyaz Belgaum,Mahdi H. Miraz, Jawdat Alshaer, "Challenges of Internet of Things and Big Data Integration", Proc. of theInt. Conf. on Emerging Technologies in Computing 2018 (iCETiC '18), Part of the Lecture Notes of theInstitute for Computer Sciences, Social Informatics and Telecommunications UK,2018,pp.47-55.Available:https://link.springer.com/chapter/10.1007/978-3-319-95450-9_4.
3. Zainab Alansari, Nor Badrul Anuar, Amirrudin Kamsin, Mohammad Riyaz Belgaum, Jawdat Alshaer, Safeeullah Soomro, Mahdi H.Miraz, "Internet of Things: Infrastructure, Architecture, Security and Privacy", 2018 Int. Conf. on Computing, Electronics & Communications Engineering (iCCECE), South end, United Kingdom, 2018,pp. 150-155,doi:10.1109/iCCECOME.2018.8658516.
4. AmeerRosic,"ProofofWorkvsProofofStake:BasicMiningGuide",Blog2017.Available:https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake.
5. Shashank, "Blockchain Technology – Unfolding the Technology behind Bitcoins", Blog 2017. Available:https://www.edureka.co/blog/blockchain-technology/.
6. Mahdi H. Miraz and David C. Donald, "Application of Blockchain in Booking and Registration Systems of Securities Exchanges",Proc.of the IEEE Int. Conf. on Computing, Electronics &Communications Engineering 2018 (IEEE iCCECE '18), Southend, United Kingdom, 16-17 August 2018, pp. 35-40, doi:10.1109/iCCECOME.2018.8658726.
7. David C.Donald and Mahdi H.Miraz,"MultilateralTransparencyforSecuritiesMarketsthroughDLT",intheFordhamLawEngineering (LNICST), vol.200,London,Review,Vol.XXV,Issue1,January2020,pp.97-153.Available:https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/2/.
8. Md Mehedi Hassan Onik, Mahdi H. Miraz, and Chul-Soo Kim, "A Recruitment and Human Resource Management Technique Using Blockchain Technology for Industry 4.0",Proceeding of Smart Cities Symposium(SCS-2018), Manama,Bahrain,2018, pp.11-16. doi:10.1049/cp.2018.1371.
9. Omar Dib, Kei Leo Brousmiche, Antoine Durand, Eric Theaand Elyes Ben Hamida, "Consortium Blockchains: Overview, Applications and Challenges", International Journalon Advances in Telecommunications, vo1.no.1&2,2018,p.5164. Available:http://www.iariajournals.org/telecommunications/tele_v11_n12_2018_paged.pdf.
10. FranCasino,ThomasK.DasaklisandConstantinosPatsakis,"Asystematicliteraturereviewofblockchain-based applications: Current status, classification and open issues", Telematics and Informatics, vol. 36,March2019,pp.55-81,ISSN0736-5853, doi:10.1016/j.tele.2018.11.006,ElsevierLtd.Available:http://www.sciencedirect.com/science/article/pii/S0736585318306324.