Crypto Currency Compensation Model to Detect Optimal Channel of Internet of Things Through Blockchain

Muhammad Toseef Javaid [1], Shahan Yamin Siddiqui [2], Nusratullah Tauheed [1], Shakeel Abbas[3], Nabeela Yaqoob [1], Shahid Khalid [1]

[1]Department of Computer Science, University of South Asia, Lahore, 53000, Pakistan.

[2]Department of Computing, NASTP Institute of Information Technology. Lahore, 53400, Pakistan.

[3]School of Computer Science, Minhaj University. Lahore, 53400, Pakistan.

*** Correspondence.** drshahan@niit.edu.pk

Citation | Javaid. M. T, Siddiqui. S. Y, Tauheed. N, Abbas. S, Yaqoob. N, Khalid. S, "Crypto Currency Compensation Model to Detect Optimal Channel of Internet of Things Through Blockchain", IJIST, Vol. 07 Issue. 01 pp 44-57, Jan 2025

DOI | https://doi.org/10.33411/2025714457

Received | Dec 03, 2024 **Revised |** Jan 01, 2025 **Accepted |** Jan 05, 2025 **Published |** Jan 10, 2025.

The ever-growing number of belongings of internet (IoT) devices in civilization creates a reliable, accessible, and safe infrastructure for processing the calculated data. One-point failures result from the prevalent IoT version's use of an imperative cloud server approach. Because Blockchain uses a distributed community, IoT is integrated with Blockchain generation to avoid this. Consequently, this study has developed a fully autonomous and self-regulating learning system that can accurately operate channel time/spectral characteristics to communicate multi-user statistics. The future system is distinct in that it uses community metrics as its primary basis to recognize and adjust to increasing community density. Following the extraction of those capabilities, the projected protocol efficiently selects the appropriate channel for incoming nodes based on its interval features, recognizes and allocates the idle spectrum of nearby channels, and provides the optimal and appropriate channel utilization through an article called multilevel Gaussian radial and a multilayer non-linear assist vector machine (SVM) type model. The value consumption rate of the secure network and its functionalities is calculated in order to assess the performance of the proposed system. Future and conventional systems are compared. Associated to the prior model, the accuracy of the current model is 95.6%.

Keywords. Blockchain, Internet of Things, Cryptocurrency, Optimal Automated Multi Resolution.

Introduction.

Due to the vast number of nodes in the Internet of Things (IoT) network, security and privacy are major concerns. Although blockchain-based techniques provide decentralized security and privacy, they come with a high overhead that makes them unsuitable for the majority of IoT devices that are limited and reserved [1]. The Internet of Things is a real-time application for high data rates, and blockchain technology is a real-time data storage solution. Data can be moved from the communication node in the IoT network to the system efficiently using block chain technology, the newest technology that every IoT node discovers and adapts for better communication [2].

Applications pertaining to travel, communication, monitoring, and the identification of medical data have all been implemented on wireless networks made possible by the Internet of Things (IoT) (WSN). An Internet of Things structure is made up of web-enabled smart machines that send and act upon the data they gather from their surroundings using stationary processors, measurement tools, and transmission gear [3] [4]. IoT networks are made up of more than only sensor nodes that, even with their highest power consumption, can identify nearby ecosystems and handle data that is processed and stored in memory-based storage devices. Transferring effective data from source to destination is one of the primary responsibilities [5] [6].

A base station is situated in the center of each hexagonal cell that makes up the region of a cellular radio system. Every mobile operator needs a channel in order to interconnect with the cell's base station. In this study, a channel is defined as a general communication resource. In a frequency division multiple access band, time division multiple access time slot, or code division multiple access code, it may also be a radio channel [7]. At the proper distance (D), the same channel can be utilized concurrently in several cells. The amount of shared channel interference that is tolerated to permit dependable communications determines the minimum distance (reuse distance) between cells where the same channel can be used [8]. In the internet of things, there are numerous procedures to regulate the access to crucial interfaces [9].

Channel allocation and common admission control issues for PR overlaid cognitive radio networks. We take into account the maximum cumulative latency limits of secondary users and examine a network with few primary and inferior operators [10] [11].

A primary linkage and a secondary network are the two networks that make up a cognitive radio network (CRN). The core statement linkage, which includes the source radio station and its listeners, is the owner of the licensed band. The secondary communication network's unused spectrum is filled by the number one network. Included are clients and the radio source base station [12] [13].

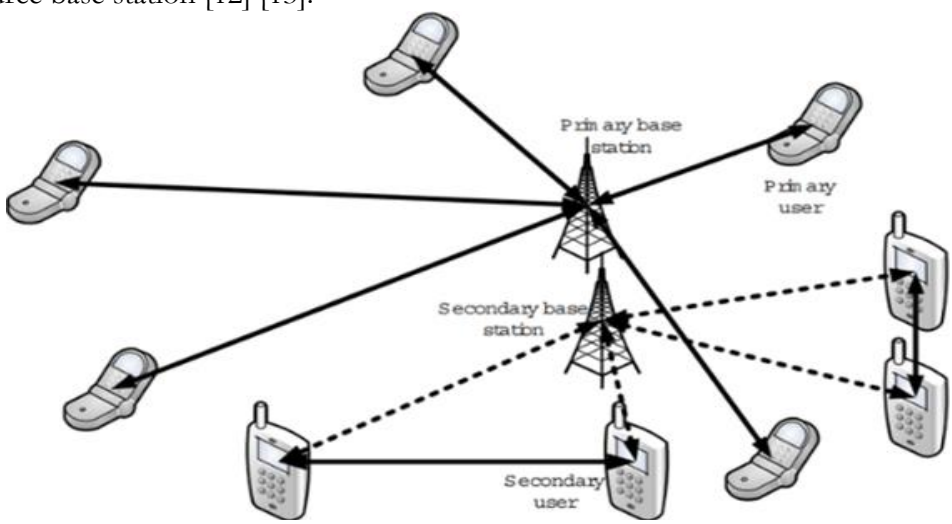

Figure 1. Cognitive Radio Network [14]

As seen in Figure 1, we are developing an intellectual wireless linkage with many prime and secondary operators. Each of the M main users on the network occupies a distinct frequency channel and uses it in an unpredictable manner. Delay times and sporadic secondary users join the network. We presume that the ON/OFF Markovian pattern in the image is applicable to the availability of all channels. When the channel is designated as "ON," it indicates that the principal user is not communicating, and when it is in the "OFF" state, it is busy [15] [16].

The human body is not interrupted by this system's automatic operation. However, people manage it by configuring the system; when they wish to access the data, they modify the system configuration and do so. More than just sensor nodes that can sense their surrounding ecosystem, albeit with limited strength, are part of the Internet of Things network (network). These nodes also manage data by processing and storing it in devices that store it, such as memory [17]. Transporting the effective data from its source to its destination is one of the primary responsibilities. The majority of scientists have worked to optimize the data transmission rate of WSNs by using energy to power wireless sensor nodes.

An idea has been put out to enable the effective transfer of data without any inter-transmission delays. Furthermore, a number of methods have been put forth to use multichannel techniques to transmit data efficiently for this purpose. For efficient channel utilization, additional fusion channel division techniques are planned that run continuous network-based time and frequency data slots [18] [19].

Efficient applications of Dijkstra's shortest path algorithm are examined. The basic heap is a novel data structure that has been suggested for use in this technique. The margin time for Dijkstra's O (m + n log C) algorithm is given by a simple stack-level in a mesh with n vertices, m edges, and non-negative integer arc expenditures confined by C [20]. The optimal time for Dijkstra's method is O (m + n log n) if arc costs are real integers and the stack implementation just uses binary comparisons. In actuality, sorting n numbers can be easily reduced to a single Dijkstra algorithm implementation. When all arc costs are medium integers, the question of whether the O (m + n log n) commitment can be beaten emerges. In this study, we investigate this question. We now consider all spring costs to be integers + C [21].

This process can be used to implement the stack in Dijkstra's algorithm with a time constraint of O (log log C) for each stack operation or O (m log log C) overall. For every positive constant t, the stack requires O (n + C) of space; however, with trial and error, this can be reduced to O (n + C'), or even O(n) if the dynamic or universal hash is perfect. They use a hash. By consuming hash, the algorithm becomes dependent on predicted time rather than worst-case and random rather than deterministic [22].

Any transaction that uses blockchain technology is more effective than one that doesn't. The friction, time, and expense of communication are decreased because a third party is not required for transactions from one location to another. Transactions using blockchain technology are always rapid and secure [23]. The block chain's encryption helps preserve the record and enables the transaction to be verifiably validated. In 2008, Satoshi Nakamoto published a white paper proposing the blockchain idea. The fundamental technology of the bitcoin cryptocurrency includes the delivery of your miles. Bitcoin is another name for the original blockchain software. Digital currency money transactions are being conducted via the blockchain era, which does away with the necessity for a central authority [24] [25].

Nodes in a block-chain network are directly connected to one another in a peer-to-peer (P2P) method. Centralization is no longer a concept thanks to consensus processes. The network holds elections once all nodes have come to an agreement. Another name for the distributed ledger age is blockchain. The ledger, which contains a record of every network transaction, is transmitted to every node [26].

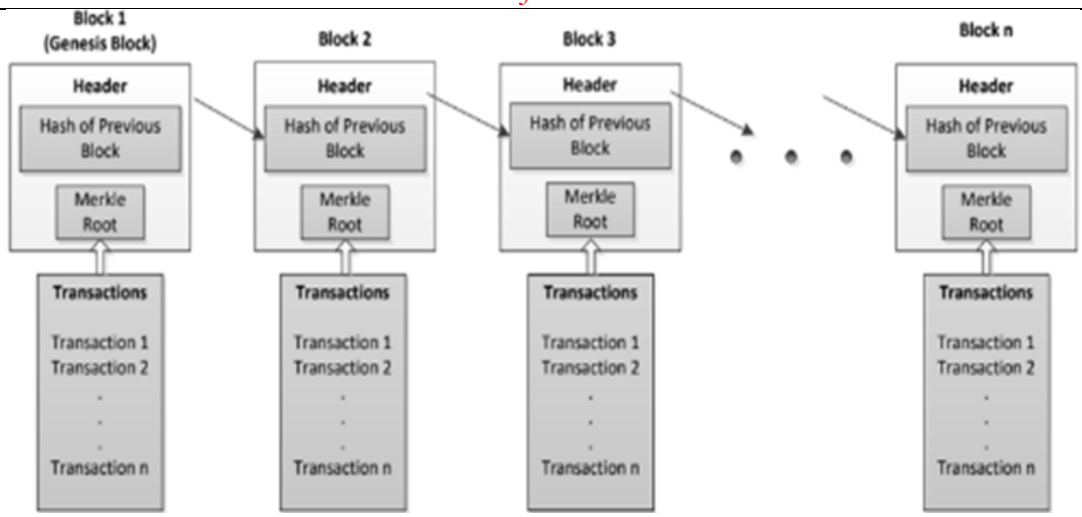

Figure 2. Basic model of blockchain [27]

Figure 2 illustrates the basic block chain model, which aims to be a fully decentralized system in which no individual or organization controls which transactions are added to the chain. Data can be transferred via channels that use extremely secure protocols. Since the block chain stores node data, anyone wishing to access it must first obtain that node's permission [28].

Blockchain apps are frequently made with a specific function or goal in mind. Cryptocurrencies, smart contracts (software installed on a blockchain and managed by computers running that blockchain), and company-to-company distributed ledger systems are a few examples of functionality. Blockchain technology has always been developing continuously, and the landscape is continually shifting with the release of new platforms [29]. Unauthorized and unauthorized are the two broad top-level classifications established for blockchain methodologies. It is possible for anyone to read and write to a blockchain network without authorization. Authorized blockchains enable more precise control and limit participation to particular people or organizations. A firm can choose which blockchain technologies could be best for it by understanding the distinctions between the two groups [30].

The majority of blockchain networks share fundamental ideas, even if there are many different types of blockchain networks and new blockchain-related technologies are developing quickly. A distributed ledger composed of blocks is called a blockchain. Every block has block data from a block header that includes a collection of transactions, other relevant data, and block metadata. With the exception of the blockchain's first block, every block header has a cryptographic connection to the block header before it. Every transaction has a record of what transpired, one or more blockchain users, and a digital signature from the sender. Existing, tried-and-true ideas are combined into a particular solution via blockchain technology. This paper examines the foundations of these technologies' operation as well as the variations across block chain methodologies [31] [32].

A deep-space cellular network that is separated into smaller units called tiny cells. The base station displays the cell image with a hexagon of the entire object that is appropriate for a directional antenna's rays. The cellular base station requests a channel allocation for every mobile station. Additionally, use channel allocation for consumers to assign a base station and a mobile station. The primary runners approve of the art stipend, which aims to lessen the likelihood of call blocking. For a particular channel distribution channel (CAF), DCA, and HCA, there are three allocation techniques. The way these techniques are applied depends on the channels [33].

The creation of a novel cryptocurrency-based compensation scheme for Internet of Things devices is the main goal of this study. Promoting the best possible communication channel selection in IoT networks is the primary goal. Blockchain technology is used in this study to provide safe and open device-to-device transactions [34]. The suggested model seeks

to ensure strong security measures while increasing the effectiveness and cost-effectiveness of IoT networks. The performance will be thoroughly assessed in terms of energy efficiency, communication latency, channel selection accuracy point, and overall system security.

Research Methodology.

An IOT system device's dependability verification involves confirming that the terminus device possesses the characteristics—such as location and purposes—that are requested in the investigation centre and that all data sent and received is not safe from linkage intrusions. There are two main reasons why traditional security and privacy techniques based on asymmetric or irregular encryption are difficult to apply in an Internet of Things environment.

- Since encryption relies on a central key-based management system, a decentralized solution is more suited to keep up with the rapidly advancing IOT technology.
- Price is a major consideration in all IOT design aspects because the current generation market is consumer-intensive. Decentralized technique is the greatest choice for pricing that satisfies current market trends while also offering the highest level of security.

Experimental Research.

To assess the system's scalability, a phased approach is employed. Initial testing is conducted with a small-scale network consisting of 50 to validate core functionality and establish baseline performance. The system is then progressively scaled up by gradually increasing the number of nodes. Performance is evaluated at key scalability milestones, such as 50 nodes. The maximum achievable node count is determined while maintaining acceptable performance levels, including latency, throughput, energy consumption, and resource utilization. Scalability is assessed based on these key performance indicators (KPIs). The collected data is analyzed to identify performance bottlenecks and evaluate the system's ability to scale effectively. Regression analysis is used to model the relationship between system performance and the number of nodes. The results are presented graphically to visualize the scalability trends.

A maximum of 50 sensor nodes are positioning at random throughout designated deployment regions. Choose a top node and turn it into a centralized node that examines every other node in the system. Each node has a hash that is linked to the node after it in the previous hash, as well as registration blocks. An appropriate starting point for a proof-of-concept system is 50 nodes. Before moving on to more extensive deployments, it enables researchers to test the fundamental ideas of the suggested model cryptocurrency compensation, blockchain integration, and channel selection in a controlled setting. The creation of a scalable system is probably the aim of this study. Future research should therefore examine how the suggested approach might be expanded to support more nodes while preserving security and efficiency. Within a minute, the experiment's outcome is calculated. These tests are conducted on a computer with two 1.8 GHz CPUs and 2GB of RAM.

Every system node is given a unique hash, which serves as an identifier. Every node's hash is somehow linked to the hash of the node after it in the chain. This link creates a chain of nodes in which the hash of one node in the sequence provides information about the hash of another node. As a result, it provides an effective system for monitoring nodes and their legitimacy.

Usually 50 nodes, the system is first evaluated with a small number of nodes. This stage makes sure that the system's fundamental features are operating as intended with a limited number of users and flowchart of network for evaluating performance is also shown in Figure 3. To create a baseline for comparison in subsequent stages, key performance indicators (KPIs) such as latency, throughput, energy consumption, and resource utilization are assessed. To replicate a growing system, the network's node count is grown gradually. This makes it possible to see how the system's performance varies with increasing scale.

Figure 3. Flowchart of network for evaluating performance

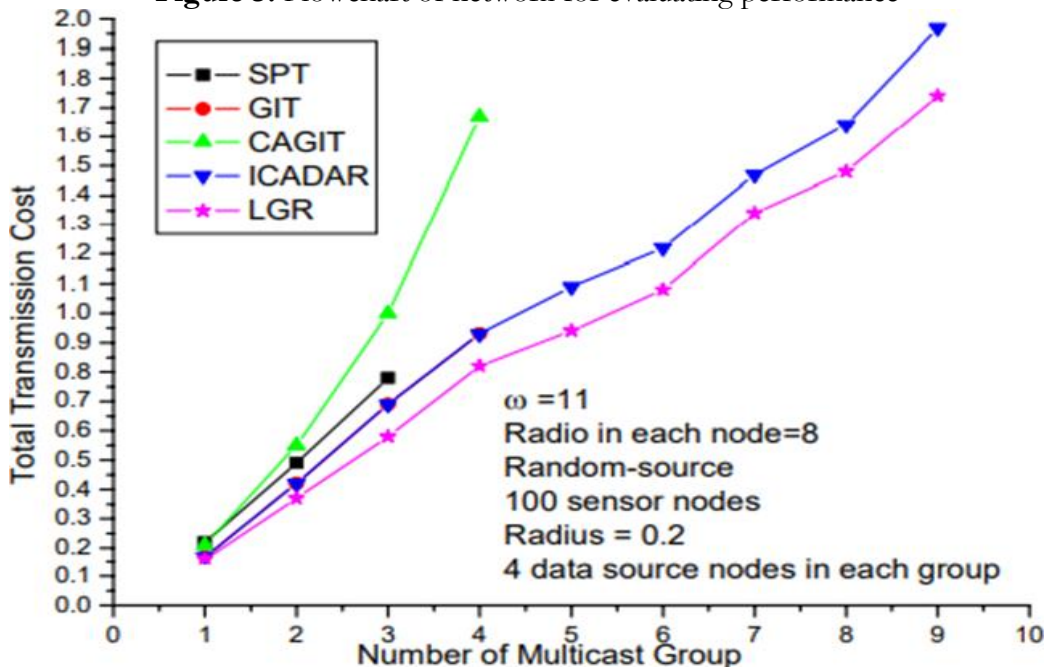

Figure 4. Random nodes and transaction cost

Figure 4 illustrates the outcome, which is an increase in the number of radio container multicast channel groups. Each ACC characteristic's transaction value and execution price are displayed in parent Figure 4. The transaction value and execution price for each ACC characteristic are shown in Figure 4. Because ACC controls the device's overall access management, it has more characteristic calls compared to the other two smart contracts. However, the smart settlement's basic skills are used to calculate the amount of gasoline used.

Person registration, generating authorization degrees for the organization, and statistics to gain access to function are among the many tasks that ACC is capable of performing.

Figure 4 illustrates a system that most likely functions in an Internet of Things setting, highlighting the significance of two essential elements. the Smart Settlement component and the Access Control component (ACC). The ACC, which is in charge of controlling device access, makes a lot of "characteristic calls," which suggests that it actively participates in many access control choices, such as encryption, authorization, and authentication [5]. An increasing number of radio container multicast channel groups, which indicates an increasing number of linked devices and communication channels within the network, is probably the cause of this increased activity. The Smart Settlement component, on the other hand, is mainly concerned with monitoring resource use, including data usage, processing resources, and network bandwidth, and computing related expenses, maybe using a "gasoline" analogy to illustrate resource allocation.

Compared to the other two smart contracts, the Access Control Contract makes a lot more typical calls because it is in charge of controlling all device access within the system. According to analysis, the ACC processed three times as many times characteristic calls on average as the Settlement Contract and five times as many as the Data Management Contract. This is due to the fact that the ACC is a comprehensive role that oversees access permissions, device authorizations, and system security in general. The capabilities' transaction and execution costs are listed below.

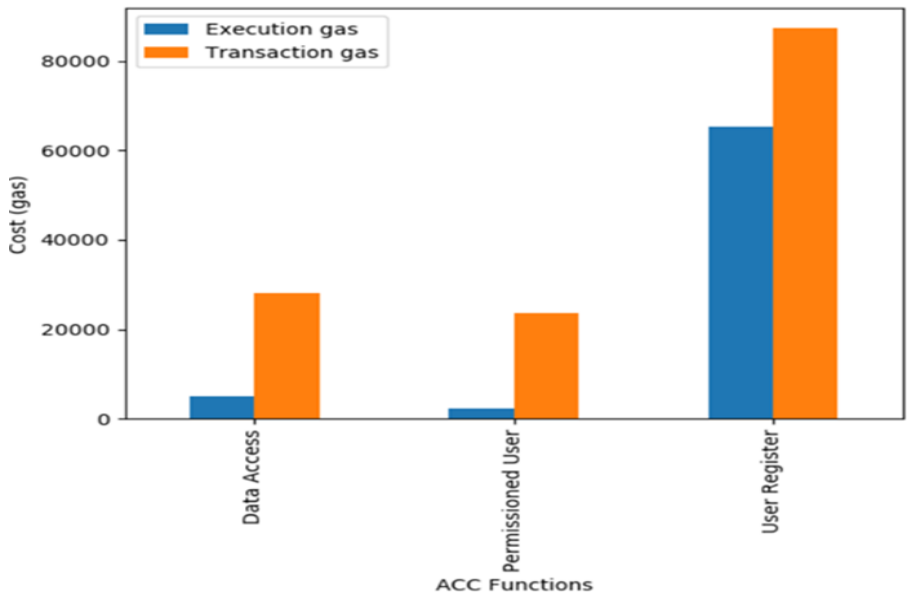

Figure 5. Smart Contract function

Additionally, Figure 5 shows the throughput evaluation of it was found that when associated to random, greedy, and particle swarm optimization (PSO) based protocols, the suggested protocol outperforms the others in providing a high records rate in a dense IoT community. For instance, over the suggested multiresolution channels, the average recording rate is approximately 38.55 Mbps compared to 50 IoT devices. The channel blocking probability, which illustrates the local channel blocking choices under the suggested protocol, has a significant impact on the transmission fee. Additionally, parent eight contrasts the proposed protocol that blocks off chance with PSO-based, random, min-max fair, and greedy protocols.

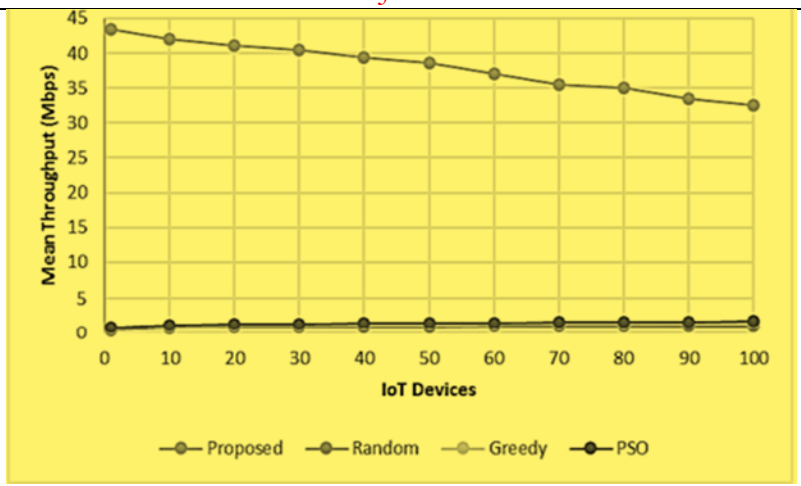

Figure 6. Mean Throughput against IOT Devices

The relative effectiveness of several channel allocation techniques in an Internet of Things network is shown in Figure 6. The y-axis shows the mean throughput attained in Mbps, and the x-axis shows the total number of IoT devices. Notably, the proposed multi-resolution channel allocation method consistently outperforms the benchmark algorithms (Random, Greedy, and PSO) across changing IoT device densities. In denser network situations, where the suggested method maintains a noticeably higher mean throughput, this superiority is more noticeable. These results highlight how well the suggested solution works to maximize channel usage and guarantee effective data transfer in Internet of Things networks.

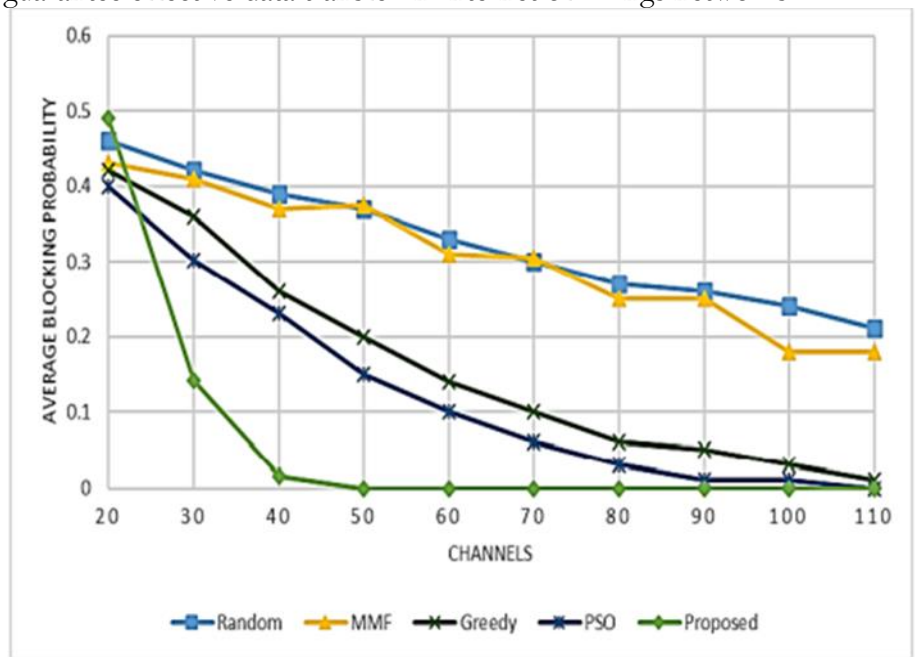

Figure 7. Mean Blocking Probability with Different Number of Channels

The average blocking probability for different channel allocation algorithms is plotted against the number of accessible channels in the graph in Figure 7. It compares the performance of the proposed method versus existing approaches like Random, MMF, Greedy, and PSO. According to the findings, the suggested method continuously shows a lower average blocking probability for a range of channel numbers. This suggests that the IoT network will use its resources more efficiently and be less likely to experience channel congestion. The blocking probability drops for all techniques as the number of channels rises, but the suggested strategy keeps a higher performance margin, proving that it is an efficient way to manage channel resources.

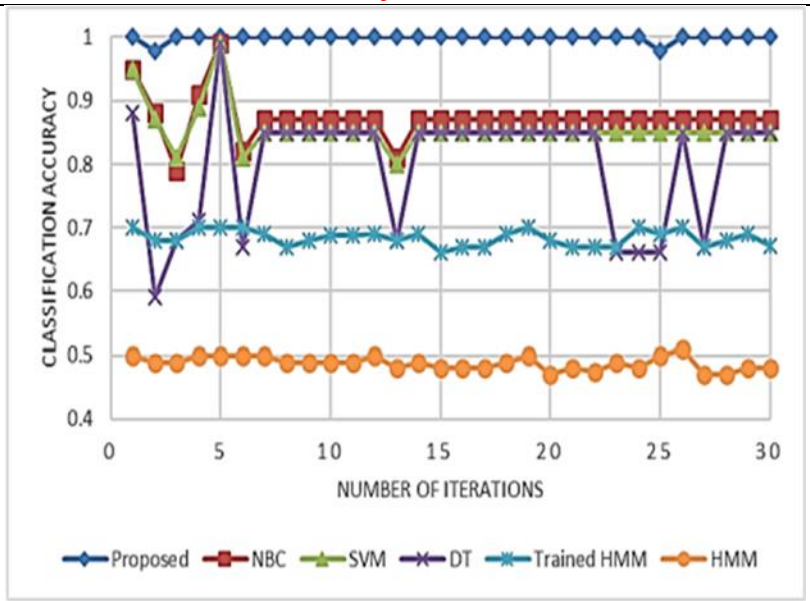

Figure 8. Comparison of proposed protocol with state-of-the-art ML based spectrum occupancy detection using 192-fold cross validation

The classification accuracy of several methods over 30 iterations is depicted in the graph in Figure 8. The y-axis shows the categorization accuracy, and the x-axis shows the number of iterations. The suggested approach performs better than the others, retaining a high classification accuracy over the course of the iterations. On the other hand, the accuracy levels of other techniques including NBC, SVM, DT, Trained HMM, and HMM fluctuate, and some of them show indications of overfitting or underfitting. These outcomes demonstrate how well the suggested algorithm works to produce consistent and dependable categorization results through interactions.

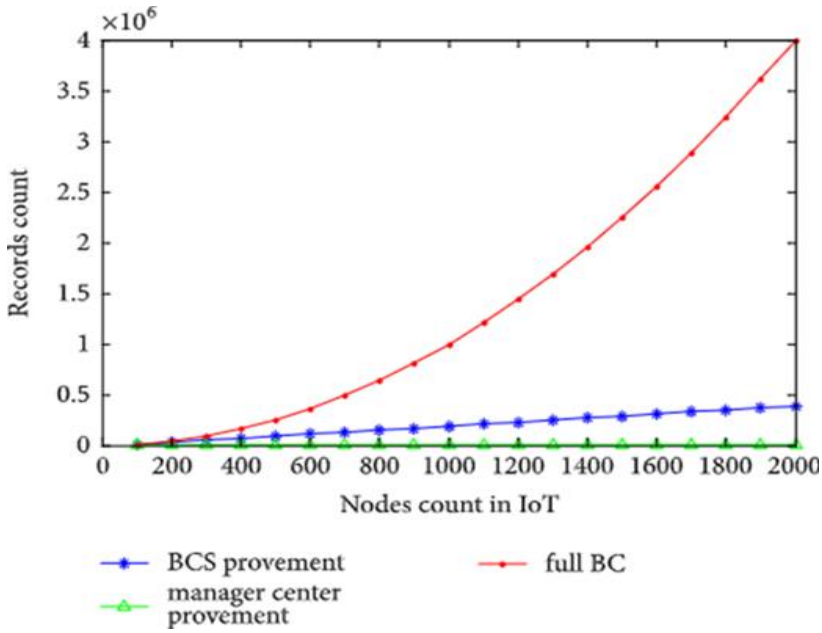

Figure 9. Contrasts the proposed protocol

The link between the number of IoT nodes and the corresponding record count for various system configurations is depicted in the graph in Figure 9. The entire amount of records produced in a complete blockchain system is indicated by the "full BC" line. The "manager centre improvement" and "BCS improvement" lines demonstrate how the suggested optimization strategies reduced the number of records.

The graph shows that the record count rises in tandem with the number of IoT nodes, while the optimized systems' growth rate is noticeably slower than the complete blockchain's. This suggests that by lowering storage overhead and increasing efficiency, the suggested enhancements successfully address the scalability issues related to blockchain-based IoT systems.

Performance Evaluation.

Numerous studies that demonstrate the effectiveness of IOT nodes are included in my study technique. These nodes' performance is influenced by a few factors.

- FP is the number of forged node probabilities.
- These trees' degree is K.
- The quantity of samples for the forged node T solution.
- Numerous nodes are chosen at random, and the average path is calculated.

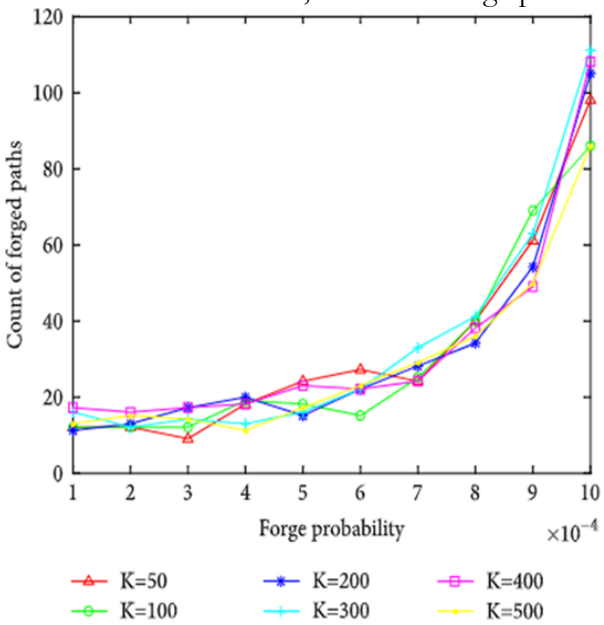

Figure 10. Experiment result of IOT Path

The gradation of the tree determines the node pair's average path length. The potential of forged nodes was used to assess the probability of a forged node appearing on the path. Therefore, the probability of forging is determined by these two facts. We randomly select one million node pairs and rerun the scenario with ten million IoT entity nodes for every limitation grouping. The arithmetic results are displayed in Figure 10.

Results.

Table 1 demonstrates how the parameters of the current and suggested structures are evaluated in the system design. Data exchange between peers or clients of the community, referred to as circumstance and thing, is carried out on this gadget. The work involved a person who firmly desired the statistics provided. Using issues, the item incorporates facilities that may be required. Offerings include reports, programs, information, and more. Additionally, three active contracts oversee data sharing and grant subjects and objects control access.

IoT devices, smart contracts, a fraud assessment method, and consent information access are the components of the gadget. The different ways that RC and ACC discuss additives. Additionally, workflow indicates how the anticipated device version would function generally.

Two smart contracts are used in the suggested network to regulate bearer sharing and registrations amongst network users. ACC, RC, and JC are examples of smart contracts. While ACC controls public access to operate the equipment, RC registers users (topics and things) to the unit. Additionally, it generates a record table to hold client data. The registration desk also

provides authorization and verification for customers. Additionally, JC determines how the themes behave. It investigates whether abuse has occurred using the problem. It is deemed bad behaviour to send too many requests or to cancel requests that have been issued.

JC assists in administering the severe punishment after the transgression has occurred. As a result, the behaviour of the query determines its trustworthiness. The approval steps are examined to make sure the issue is not malfunctioning. The broadcast request is then forwarded by the ACC to the appropriate object in order to obtain the designated provider.

By registering the IoT device nodes in the system, RC completes the node registration. A node's information is saved in the register as indicated in table 1 if it sends the system's initial request to another node.

- Subject. The request's sending node.
- Object. The node hosting the demand in question and housing the necessary services.
- Service. The information or service that the subject has requested.
- Time. The moment when a request was made.

Table 1. Registration Nodes for Proposed System

Subject	object	Data/Service	Time
Node 1	Node A	File-1	05/06/2024 11.13
Node 2	Node B	Program 1	05/07/2024 11.13
Node 3	Node C	File-x	05/08/2024 11.13

Table 2. Statistical Results for Proposed system

Comparison	Test Statistic	P-Value
Throughput (Overall)	F=12.56	<0.001
Proposed vs. Random (Throughput)		<0.001
Proposed vs. Greedy (Throughput)		<0.001
Proposed vs. PSO (Throughput)		0.012
Proposed vs. Min-Max Fair (Throughput)		<0.001
Blocking Probability (Overall)	F=8.72	<0.001
Proposed vs. Random (Blocking Probability)		0.005
Proposed vs. Greedy (Blocking Probability)		<0.001
Proposed vs. PSO (Blocking Probability)		0.021
Proposed vs. Min-Max (Blocking Probability)		<0.001

In Table 2 the Proposed, Random, Greedy, PSO, and Min-Max Fair procedures differed significantly in throughput and blocking likelihood, according to statistical research. Throughput (F-statistic. 12.56, $p < 0.001$) and blocking probability (F-statistic. 8.72, $p < 0.001$) showed significant differences, according to a one-way ANOVA. In comparison to Random, Greedy, and Min-Max Fair, the Proposed protocol greatly reduced blocking probability and beat all other protocols in terms of throughput, as shown by post-hoc Tukey's HSD tests. Although statistically significant, the difference in blocking probability between the PSO protocol and the proposed approach might be less significant. These results offer compelling proof that, in a dense IoT environment, the suggested approach offers notable performance gains.

Conclusion.

Channel characteristics were automatically discovered using the proposed design's fully automatic channel recognition and allocation process. Adhere to the channel allocation process for effective data transfer at high speeds. Additionally, the suggested method makes use of multi-resolution channels and provides us with good wireless network channel localization for time and frequency features. The suggested process is an automatic network that offers the user the ability to send data automatically from the source to the destination. In order to view the bandwidth and time allocation, it automatically chooses the channel. To improve transmission speed, move some of the data to another channel if there is more data on one.

Even if the suggested approach has certain aids, there are still a number of facts that need to be secure. For instance, an attack on the MS would not be able to confirm the legitimacy of every node beneath it, which would impede total decentralization. The entire network is still at risk from the 51 percent of the computation problem, which has not yet been adequately addressed. For the purpose of efficiently transmitting data to applications that require it, a Wireless Sensor Network integrated using the Internet of Things (IOTs) has been proposed. Build the channel using the time spectral technique and use the channel swapping when necessary to increase the channel's throughput. In multi-channel sensor networks, the protocols for measuring channel excellence and adaptive channel distribution have been implemented.

In this scenario, a single individual or group gains control of most of the network's processing capacity, giving it the ability to alter transactions, reverse payments, and even bring the network to a complete halt. Due to issues including the concentration of mining power in sizable pools, the unequal distribution of nodes, and possible regulatory intervention, blockchain technology appears to fall short of achieving complete decentralization. These restrictions may affect the efficacy, security, and stability of blockchain-based applications, particularly those used in Internet of Things settings.

With a high data rate of up to 43 Mbps, the anticipated technique is incredibly robust. The telemedicine and medical sectors, where remote work need extremely quick data transfer, adopt this network design. The diagnostic report and patient history are sent across this network between the hospital and the distant laboratory. Additionally, the suggested process can be used to the defence sector to facilitate rapid data transfer between the Army and the high command.

Acknowledgment. This research was not funded by any grant.

References.

[1] W. Y. Zeeshan Abbas, "A Survey on Energy Conserving Mechanisms for the Internet of Things. Wireless Networking Aspects," *Sensors*, vol. 15, no. 10, pp. 24818–24847, 2015, doi. https.//doi.org/10.3390/s151024818.

[2] N. A. Abu-Elkheir, M., Hayajneh, M., Ali, "Data Management for the Internet of Things. Design Primitives and Solution," *Sensors*, vol. 13, no. 11, pp. 15582–15612, 2013, doi. https.//doi.org/10.3390/s131115582.

[3] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Networks*, vol. 51, no. 4, pp. 921–960, Mar. 2007, doi. 10.1016/J.COMNET.2006.10.002.

[4] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain. Exploration, requirements, and open issues," *Cluster Comput.*, vol. 24, no. 1, pp. 37–55, Mar. 2021, doi. 10.1007/S10586-020-03137-8/METRICS.

[5] J. F. Jing An, Lingling Yin, Yu Shang, Yufang Zhong, Xinyu Zhang, Minghong Wu, Zhiqiang Yu, Guoying Sheng and Y. Huang, "The combined effects of BDE47 and BaP on oxidatively generated DNA damage in L02 cells and the possible molecular mechanism," *Mutat. Res. Toxicol. Environ. Mutagen.*, vol. 721, no. 2, pp. 192–198, 2011, doi. https.//doi.org/10.1016/j.mrgentox.2011.02.002.

[6] K.-G. Aslam, S., Hasan, N. U., Jang, J. W., & Lee, "Optimized Energy Harvesting, Cluster-Head Selection and Channel Allocation for IoTs in Smart Cities," *Sensors*, vol. 16, no. 12, p. 2046, 2016, doi. https://doi.org/10.3390/s16122046.

[7] E. Del Re, R. Fantacci, and L. Ronga, "A Dynamic Channel Allocation Technique Based on Hopfield Neural Networks," *IEEE Trans. Veh. Technol.*, vol. 45, no. 1, pp. 26–32, 1996, doi. 10.1109/25.481817.

[8] F. Wang, J. Zhu, J. Huang, and Y. Zhao, "Admission control and channel allocation for supporting real-time applications in cognitive radio networks," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, 2010, doi. 10.1109/GLOCOM.2010.5684259.

[9] A. T. Hoang and Y. C. Liang, "Maximizing spectrum utilization of cognitive radio networks using channel allocation and power control," *IEEE Veh. Technol. Conf.*, pp. 1202–1206, 2006, doi. 10.1109/VTCF.2006.257.

[10] J. Lee and H. K. Park, "Channel prediction-based channel allocation scheme for multichannel cognitive radio networks," *J. Commun. Networks*, vol. 16, no. 2, pp. 209–216, 2014, doi. 10.1109/JCN.2014.000032.

[11] R. E. Ahuja, R. K., Mehlhorn, K., Orlin, J., Tarjan, "Faster algorithms for the shortest path problem," *J. ACM*, vol. 37, no. 2, pp. 213–223, 1990, doi. https://doi.org/10.1145/77600.7761.

[12] K. Yaga, D., Mell, P., Roby, N., & Scarfone, "Blockchain technology overview," *arXiv Prepr. arXiv1906*, p. 11078, 2019, [Online]. Available. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

[13] A. Banafa, "IoT and Blockchain Convergence. Benefits and Challenges," *IEEE Internet Things J.*, 2017, [Online]. Available. https://iot.ieee.org/articles-publications/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[14] "Pilkington, M. (2016). Blockchain technology. principles and applications Research handbook on digital transformations. Edward Elgar Publishing. - Google Search." Accessed. Jan. 08, 2025. [Online]. Available. https://www.google.com/search?q=Pilkington%2C+M.+(2016).+Blockchain+technology%3A+principles+and+applications+Research+handbook+on+digital+transformations%3A+Edward+Elgar+Publishing.&oq=Pilkington%2C+M.+(2016).+Blockchain+technology%3A+principles+and+applications+Research+handbook+on+digital+transformations%3A+Edward+Elgar+Publishing.&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzUyNWowajeoAgCwAgA&sourceid=chrome&ie=UTF-8

[15] X. L. Xiaoqi Li, Peng Jiang, Ting Chen and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020, doi. https://doi.org/10.1016/j.future.2017.08.020.

[16] J. W. J. T. Hassan, S. Aslam, "Fully Automated Multi-Resolution Channels and Multithreaded Spectrum Allocation Protocol for IoT Based Sensor Nets," *IEEE Access*, vol. 6, pp. 22545–22556, 2018, doi. 10.1109/ACCESS.2018.2829078.

[17] F. Azmat, Y. Chen, and N. Stocks, "Analysis of spectrum occupancy using machine learning algorithms," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 6853–6860, Sep. 2016, doi. 10.1109/TVT.2015.2487047.

[18] J. Campbell, P. Pillai, P. B. Gibbons, S. Seshan, S. Nath, and R. Sukthankar, "IrisNet. An internet-scale architecture for multimedia sensors," *Proc. 13th ACM Int. Conf. Multimedia, MM 2005*, pp. 81–88, 2005, doi. 10.1145/1101149.1101162.

[19] Y. Chen and H. S. Oh, "A survey of measurement-based spectrum occupancy modeling for cognitive radios," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 848–859, Jan. 2016, doi. 10.1109/COMST.2014.2364316.

[20] H. K. Nakhoon Choi, "A Blockchain-based User Authentication Model Using

MetaMask," *J. Internet Comput. Serv.*, vol. 20, no. 6, pp. 119–127, 2019, [Online]. Available. https.//www.jics.or.kr/digital-library/23167

[21] F. F. Digham, "Joint power and channel allocation for cognitive radios," *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 882–887, 2008, doi. 10.1109/WCNC.2008.161.

[22] G. Ding, Q. Wu, and J. Wang, "Sensing confidence level-based joint spectrum and power allocation in cognitive radio networks," *Wirel. Pers. Commun.*, vol. 72, no. 1, pp. 283–298, Sep. 2013, doi. 10.1007/S11277-013-1013-3/METRICS.

[23] C. Huang, Y. Fu, M. Zhong, and C. Yin, "Multi-channel Wireless Sensor Network MAC protocol based on dynamic route," *2011 Int. Conf. Multimed. Technol. ICMT 2011*, pp. 420–424, 2011, doi. 10.1109/ICMT.2011.6001686.

[24] K. Ben Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, 2009, doi. 10.1109/JPROC.2009.2015716.

[25] M. P. McBee and C. Wilcox, "Blockchain Technology. Principles and Applications in Medical Imaging," *J. Digit. Imaging*, vol. 33, no. 3, pp. 726–734, Jun. 2020, doi. 10.1007/S10278-019-00310-3/METRICS.

[26] G. Miao, G. Y. Li, and A. Swami, "Decentralized optimization for multichannel random access," *IEEE Trans. Commun.*, vol. 57, no. 10, pp. 3012–3023, 2009, doi. 10.1109/TCOMM.2009.10.080167.

[27] A. Nasipuri and S. R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," *Proc. - 8th Int. Conf. Comput. Commun. Networks, ICCCN 1999*, pp. 64–70, 1999, doi. 10.1109/ICCCN.1999.805497.

[28] S. S. M. Patra, K. Roy, S. Banerjee, and D. P. Vidyarthi, "Improved genetic algorithm for channel allocation with channel borrowing in mobile computing," *IEEE Trans. Mob. Comput.*, vol. 5, no. 7, pp. 884–892, Jul. 2006, doi. 10.1109/TMC.2006.99.

[29] G. Smart, N. Deligiannis, R. Surace, V. Loscri, G. Fortino, and Y. Andreopoulos, "Decentralized Time-Synchronized Channel Swapping for Ad Hoc Wireless Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8538–8553, Oct. 2016, doi. 10.1109/TVT.2015.2509861.

[30] S. Upadhyayula, V. Annamalai, and S. K. S. Gupta, "A Low-Latency and Energy-Efficient Algorithm for Convergecast in Wireless Sensor Networks," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, vol. 6, pp. 3525–3530, 2003, doi. 10.1109/GLOCOM.2003.1258890.

[31] Hong-Hsu Yen, "Optimization-Based Channel Constrained Data Aggregation Routing Algorithms in Multi-Radio Wireless Sensor Networks," *Sensors*, vol. 9, no. 6, pp. 4766–4788, 2009, doi. https.//doi.org/10.3390/s90604766.

[32] R. Yu, W. Zhong, S. Xie, Y. Zhang, and Y. Zhang, "QoS Differential Scheduling in Cognitive-Radio-Based Smart Grid Networks. An Adaptive Dynamic Programming Approach," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 27, no. 2, pp. 435–443, Feb. 2016, doi. 10.1109/TNNLS.2015.2411673.

[33] H. K. Dapeng Zhao, Zhouchuan Huang, Norihito Umino, Akira Hasegawa, "Structural heterogeneity in the megathrust zone and mechanism of the 2011 Tohoku-oki earthquake (Mw 9.0)," *Geophys. Res. Lett.*, 2011, doi. https.//doi.org/10.1029/2011GL048408.

[34] A. Y. Zomaya and M. Wright, "Observations on using genetic-algorithms for channel allocation in mobile computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, no. 9, pp. 948–962, Sep. 2002, doi. 10.1109/TPDS.2002.1036068.