A Proposal for Designing a Novel Blockchain-Based Data Provisioning Mechanism for IoT Integration in Smart Applications

Hussein Al-Rammahi [1], Ameer Yalmaz Asaad [2]
[1] Electrical and Computer Engineering, Altinbas University, Istanbul, Türkiye
[2] Istanbul Topkapi University, Plato Vocational School, Department of Computer Technologies, Computer-Aided Design and Animation Program, Istanbul, Türkiye
Email: [1] hussienmoho@gmail.com, [2] emirgul@topkapi.edu.tr
Corresponding Author

***Abstract*—The Internet of Things (IoT) presents unique communication and security challenges due to the diverse nature and sheer volume of connected devices. Traditional communication solutions are often insufficient to meet these demands. This paper addresses the critical need for robust security in IoT by proposing a novel, blockchain-based mechanism for secure data provision in smart applications. While security is frequently overlooked in IoT in favor of application and hardware development, distributed ledger technology (blockchain) offers a promising solution. Beyond its role in cryptocurrencies, blockchain offers inherent capabilities for device identity, secure data transfer, and immutable data storage, all within a decentralized and transparent system that provides auditable cryptographic proofs. This paper aims to thoroughly analyze blockchain technology and evaluate prominent frameworks such as Ethereum and Bitcoin. We will examine the distinct features and target use cases of these frameworks to determine the most suitable blockchain architecture for the IoT ecosystem. This paper provides a high-level comparison of the evaluated architectures, alongside sample use cases and ongoing research, to aid developers and managers in selecting an appropriate framework based on their specific application requirements. The core contribution is the design and initial validation of our novel mechanism, which enhances data integrity and trust within IoT environments.**

***Keywords*—Blockchain, Internet of Things, Smart Applications, Styling, Cryptocurrency**

I. INTRODUCTION

In the digital age, the Internet of Things (IoT) has become a disruptive force that is changing how we engage with both technology and the real world. The Internet of Things (IoT) is a network of linked devices that are embedded with sensors and software. These devices can communicate and share data to carry out tasks either independently or in conjunction with other systems. Applications for this networked ecosystem are numerous and include everything from industrial automation and environmental monitoring to smart homes and healthcare systems [1], [2].

Improvements in connectivity, sensor miniaturisation, and the combination of cloud computing and data analytics are driving the Internet of Things' explosive growth. Large volumes of real-time data can now be gathered, processed, and analysed, creating new opportunities for process optimisation, better decision-making, and enhanced user experiences. Although the Internet of Things has great potential, there are a number of obstacles to its widespread adoption, such as worries about data privacy, security, and compatibility across various platforms and devices [3].

Fig. 1 presents the architecture of the Internet of Things (IoT), which is structured into five distinct layers, each serving a specific function within the IoT ecosystem. The Perception Layer constitutes the lowest layer and is primarily responsible for sensing and gathering data from the surrounding environment through various sensors. This data collection forms the basis for further processing and analysis. The Transport Layer is crucial for the efficient and reliable transmission of sensed data between various components and layers within an IoT system. This layer leverages a diverse array of network protocols, with selection rigorously determined by specific application requirements concerning communication range, power consumption constraints, desired data rate, and critical real-time performance needs. For instance, short-range wireless technologies such as Bluetooth, RFID, and Near Field Communication (NFC) are typically employed for localized data exchange. These are ideal for scenarios like device pairing, proximity-based interactions (e.g., smart payments or access control), or sensor networks operating within a confined area. Their appeal lies in their low power consumption, cost-effectiveness, and ability to support high spatial device density. In contrast, longer-range protocols, including 3G/4G/5G cellular networks, Wi-Fi (WLAN), and wired Local Area Networks (LAN), are utilized for broader coverage, higher data throughput, and more extensive network integration. These are essential for applications requiring continuous, wide-area connectivity, such as smart city infrastructure, remote asset tracking, or industrial IoT deployments across large facilities. The strategic design and choice of transport-layer protocols critically impact the overall latency, scalability, and real-time responsiveness of the entire IoT architecture. For example, protocols optimized for minimal overhead and rapid data transmission contribute significantly to reduced latency, which is absolutely essential for time-sensitive applications like autonomous vehicles, remote surgery, or critical infrastructure monitoring where even milliseconds of delay can have severe consequences. Similarly, highly scalable transport solutions are necessary to gracefully accommodate the massive and ever-growing volume of data generated by a proliferating number of IoT

devices without compromising network stability, bandwidth, or performance. Therefore, a thorough and careful consideration of these intricate factors during protocol selection is paramount to ensuring seamless, efficient, robust, and truly responsive data flow throughout the entire IoT ecosystem, directly influencing the reliability and effectiveness of the end-to-end solution [4].

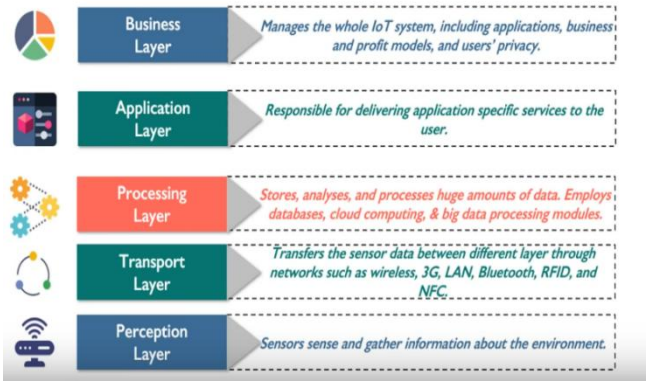

Fig. 1. Architectural layers of the IoT system

At the core of the IoT architecture, the Processing Layer manages the enormous volumes of data accumulated by the Perception Layer. It employs advanced techniques in data storage, analysis, and processing, leveraging tools such as databases, cloud computing, and big data processing modules to extract meaningful insights from raw data. The Application Layer is responsible for delivering domain-specific services to the end user. It ensures that the processed data is applied to meet the practical needs of various applications within the IoT framework. Finally, the Business Layer is tasked with the overarching management of the IoT system, including the orchestration of business processes, application functionalities, profit models, and the protection of user privacy. This layer ensures that the IoT system operates within the defined business and legal frameworks, aligning technological capabilities with organisational objectives. Collectively, these layers form the backbone of IoT systems, ensuring effective data collection, transmission, processing, and application, while maintaining secure and efficient operations [5]-[10].

The decentralised and distributed ledger system known as blockchain technology has drawn a lot of interest due to its potential to solve some of the problems that come with Internet of Things networks. Fundamentally, blockchain eliminates the need for a central authority by enabling safe, open, and unchangeable record-keeping. To create a chronological and impenetrable history, every transaction or piece of data is grouped into blocks and added to a chain of earlier records. Because of its structure, blockchain is especially well-suited for applications where data integrity, security, and trust are crucial [11].

Blockchain has the potential to significantly improve the security and dependability of networked devices in the context of the Internet of Things. The susceptibility of IoT networks to cyberattacks, including data breaches and illegal access to private devices, is one of the main worries. IoT systems may be shielded from these threats by the decentralised, cryptographically secure environment that blockchain offers. IoT devices can independently verify and carry out transactions using smart contracts, which are self-executing contracts with the terms of the agreement directly encoded into lines of code. This ensures that data exchanges are precise, safe, and impenetrable [12].

Additionally, the problem of interoperability in IoT networks is addressed by blockchain's decentralised structure. A centralised system may result in bottlenecks and single points of failure when a wide range of platforms and devices are interacting with one another. By ensuring that data can be accessed and verified by all network participants without depending on a central authority, blockchain's distributed ledger improves the scalability and resilience of Internet of Things systems. By merging the advantages of blockchain technology and the Internet of Things, we can open up new application opportunities in sectors like finance, healthcare, supply chain management, and smart cities. Blockchain provides a safe, transparent way to track and store the vast amounts of data generated by IoT devices in a way that ensures its authenticity. The combination of blockchain technology and the Internet of Things promises a more decentralised, safe, and effective digital future [13].

This paper uses a thorough methodology to investigate how blockchain technology can be integrated with the IoT. In order to comprehend how blockchain technology can offer secure data transfer, device identity, and immutable data storage without the need for a centralised authority, a thorough investigation of the technology will first be carried out. The study will concentrate on examining important blockchain frameworks, such as Ethereum, Bitcoin, and Litecoin, paying close attention to their distinct characteristics and related applications. Assessing each framework's suitability for Internet of Things applications while taking important aspects like security, scalability, and decentralisation into account is a crucial part of this methodology. In order to help managers and developers choose the best framework for their unique IoT requirements, a comparative study of the chosen blockchain architectures will be provided. Each architecture's current research and sample use cases will also be covered, giving their application a practical context. This approach seeks to advance knowledge of blockchain's function in the Internet of Things ecosystem and facilitate the creation of safe, effective smart applications.

II. Literature Review

The rapid advancement of technology has given rise to a new era of connectivity, where everyday objects are becoming increasingly integrated into the digital world. This transformation, driven by the IoT, has revolutionised industries by enabling seamless communication between devices and providing new opportunities for automation and data analysis. With the proliferation of affordable smart devices and ubiquitous internet access, IoT applications are now pervasive across various sectors, from healthcare to transportation. As a result, industries are experiencing enhanced efficiency, improved decision-making, and a more interconnected world. However, while the benefits are undeniable, challenges such as security concerns, data management, and interoperability still need to be addressed to fully unlock the potential of IoT. Several studies have been presented in the literature, some of which are reviewed as follows:

The Internet of Things is the global network of intelligent and connected devices utilising Wi-Fi capabilities and sensors. Embedding electronics into physical objects builds some intelligence into them, making them "smart," thereby enabling these devices to communicate with each other as mentioned in [14]. These devices can range from industrial control systems, automobiles, wearable devices, medical equipment, smart home devices, and smart energy management devices. In this manner, the predictable channels of an information system are rapidly changing, and the physical world is becoming increasingly smart. The steep rise in the number of connected devices can be attributed to the ubiquitous broadband internet, low connection costs and availability of a large number of smart devices as mentioned in [15]. The following are a few applications of IoT which throw light on the advancements in wireless network technologies and the extent to which they can be leveraged for the purpose of automation and control, information analysis. Rental cars with embedded sensors provide the customers with the flexibility to pick up cars from pickup spots and return them, rather than having rental centres. The embedded sensors help in tracking the car, the distance travelled, and the rental duration [16]. The sensors in retail membership cards retrieve the shopper's data and apply the appropriate discounts at the point of sale. Aeroplane manufacturers are considering building the airframes with embedded sensors which send important data regarding the health of the critical components to monitoring systems [16]. This can help mitigate unprecedented downtime and also provide scope for proactive maintenance. For instance, in many manufacturing industries, the paper industry demands manual adjustments of temperature for lime kilns, which can be automated through the use of sensors and also, and they are also networked to alert the operators in case the temperature rises beyond the threshold [17].

The three main layers of the architecture shown in Fig. 2, the management information layer, the system control layer, and the edge device layer, represent a tiered approach for an Internet of Things-based system. At the top, the management information layer serves as the main communication hub, where tools like firewalls, routers, and identity authentication systems guarantee safe and effective data flow management. Through elements like the public history server, remote access server, and office terminal, this layer communicates with external networks, including the Internet [18]. The architecture's central system control layer is where PLCs (programmable logic controllers) communicate with control mechanisms like servers, switches, and operator stations to enable real-time operations and system monitoring. Intrusion detection systems are another component of this layer that, by spotting possible breaches, help improve security management [19]. Finally, the physical devices, such as controllers, collectors, and actuators, that have direct interactions with the environment are included in the edge device layer. By transforming data into actionable insights and powering the automation processes that maximise system operations, these edge devices serve as the interface between the digital and physical worlds. In addition to addressing important issues like system security and data management, which are essential for successful IoT deployments, this tiered structure guarantees the effective handling of data [20].

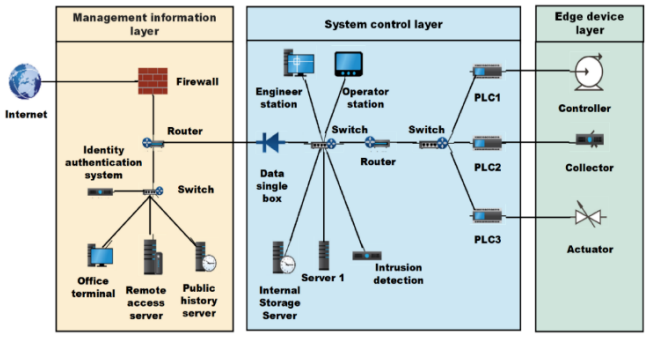

Fig. 2. Typical architecture of layered industrial internet system

Blockchain system uses encryption technology to protect data and relies on strong consistent algorithm to resist external attacks [21]. Merkle tree and its commonly used variants in blockchain systems support simplified payment verification and improve the efficiency of blockchain operation, which makes it possible to use blockchain technology on industrial internet devices. IIoT mainly applies instrumentation, sensors, and edge devices to machinery, vehicles in the transport, and the energy and industrial sectors [22]. Combined with blockchain technology, industrial control system can benefit from low operating cost, decentralized resource management, robustness against threats and attacks, etc. By allocating computing and storage requirements among all devices in the network, blockchain establishes a peer-to-peer network, which reduces the installation and maintenance costs of centralized cloud, data center and network devices. This communication mode addresses the issue of single point failure [23]. Blockchain solves the privacy problem of Internet of Things by using encryption algorithm. It also resolves the reliability problem in the IoT using tamper proof ledgers [24]. However, numerous academic literatures and some research on blockchain-based IIoT technology has only focused on general applications of the blockchain [25]-[30]. They have no insight into the blockchain challenges associated with the Internet of Things. Arias et al. [31] emphasize various security, privacy and performance problems of blockchain application in the field of IoT. Nevertheless, IoT has different multi-layer network architecture from the IIoT. Makhdoom et al. [32] put forward a lightweight architecture of the smart home and proposes a way to reduce computing density and transmission delay solutions to problems such as lateness and scalability. The effect of its practical application is not considered in depth. Dorri et al. [33] propose a scheme for configuring and managing IoT devices using blockchain smart contracts. Solve the security and synchronization problems in the terminal server model. In the IIoT environment, network nodes do not necessarily trust each other. Encryption hash link and distributed consistency mechanism ensure that the data stored on the immutable blockchain will not be changed or deleted, but the blockchain mechanism does not guarantee the reliability of the data in the source. Wang et al. [34] puts forward a cloud-edge computing framework for Cyber-Physical-Social Services. Therefore, some recent researches focus on integrating trust mechanism and performance optimization into blockchain-based IIoT applications. However, due to the inherent characteristics of industrial internet, such as lack of central

control, heterogeneous devices and limited computing capacity, traditional blockchain technology and data security protection has challenges, such as [35]-[40]:

- Resources constraints: Industrial internet consists of numerous terminal devices, which need to communicate with each other in time. However, most devices have limited resources, including bandwidth, computing and memory. This requires increasing many blocks containing a large number of transactions to the blockchain every second, which requires a consistent method with low latency.
- Multi-center management: The traditional industrial internet relies on a hierarchical agent communication model, in which all devices are identified, verified and connected through the central control system. Because of the large-scale devices, the centralized server is sometimes difficult to meet the real-time interaction needs of decentralized devices. In general, IIoT has some constraint in performance requirements, and prepare to save a certain degree of data integrity in calculation and energy consumption. One way to achieve this is to relax the proof of work to reduce the calculation requirements.
- Data security: The key parameters and sensitive data in industrial internet put forward higher requirements for data privacy and security protection. The heterogeneous network structure needs to ensure the data security protection from the sensor, communication protocol and the whole process of information processing.

A distributed access control method for sensitive data has been proposed by some academics, but it adds excessive overhead and delay. In reference [41], IPSec and TLS are used to provide privacy and authentication, but because of their high computing costs, they are not appropriate for a variety of computing devices with limited resources. Their block validation and consensus mechanism run counter to what sophisticated blockchain solutions require. To enable ubiquitous computing services, the IIoT is a network of physical objects that edge devices can monitor and control. Regretfully, industrial internet applications frequently assign tasks to cloud computing in the management information layer because of constraints in memory, power, and computational capabilities. The number of blocks that blockchain nodes can mine is constrained in industrial internet environments due to the heterogeneous, distributed, and low-powered computing resources required to participate in block consensus. In heterogeneous networks, nodes need to agree on the timing and accuracy of transactions in recently unearthed blocks. Blockchain bifurcation may result from inconsistent blockchain copies across nodes if this agreement is not reached. The issue of high computational demands must be resolved in order to add a new block to the industrial blockchain, as shown in Fig. 3. The industrial internet of things (IIoT) infrastructure is depicted in this graphical illustration, emphasising the function of edge devices, certification servers, and cloud-based management nodes. It highlights how different devices from the industry network communicate with centralised nodes to verify blocks and add them to the blockchain, guaranteeing transaction security and consistency. Therefore, resolving the issues of high computational requirements is crucial to guaranteeing dependable and effective blockchain operations in these kinds of settings [42].

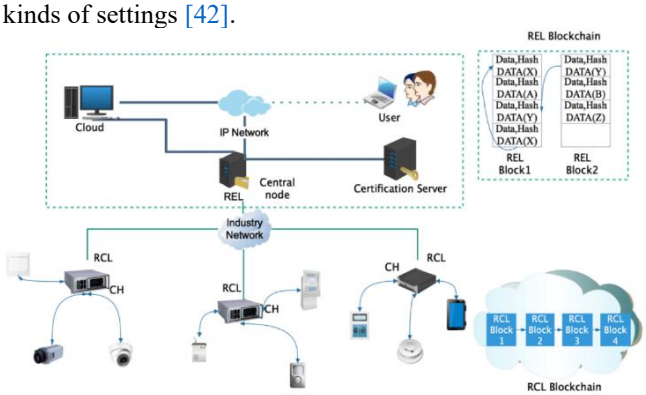

Fig. 3. Industrial IoT blockchain architecture

III. COMPARISON AND CONTRIBUTION

The integration of blockchain technology with IoT devices for smart applications presents several challenges: Firstly, unique identification for each device is crucial. Each IoT device must have a unique identifier, often achieved through a pair of cryptographic keys (public and private). However, devices such as lights or CCTV cameras may lack the capacity to manage these keys, and IP addresses are unreliable due to their dynamic nature and the use of private IPs. Secondly, the double-spending issue is resolved through mining and proof-of-work functions in blockchain, but this is particularly relevant for transactions involving monetary assets. For non-financial data transfers, there's no need to prevent double spending, though there should be a protocol in place to systematically build and append blocks to the blockchain. Another challenge is cryptographic computation; many IoT devices lack the computational power to perform the complex cryptographic calculations required for blockchain operations. With projections of 50 billion connected devices by 2022, it's important to have sufficient devices online to handle these tasks. In terms of information exchange, IoT networks involve devices that store and process diverse types of data. Managing this data within a single ledger can be cumbersome, and alternatives like sidechains might be necessary to handle different types of devices and information. Lastly, the issue of trusting devices becomes critical as more devices are added to the network. Every device has its vulnerabilities, and an attacker compromising a device could lead to a significant system breach. Therefore, blindly trusting all devices in the blockchain is risky and could lead to exploitation:

- Unique Identification for Smart Applications: Each device connected to the internet should have a unique identifier. This Id is used to track the device in the ledger. Usually, this is achieved by assigning a pair of keys (public and private) to each device. However, devices like lights and CCTV cameras might not have built-in capacity to manage these cryptography keys. IP address cannot be used for this purpose due to their dynamic nature and the presence of private IP addresses.
- Double Spending issue: Mining and proof-of-work functions are used eliminate the transactions involving double spending. This is only useful while transferring assets with monetary value. In other cases, involving the transfer of data, the same information from a device can

be sent to different devices at any time. But, there should be some protocol to build a blockchain and append blocks to it in a systematic manner.

- Cryptographic Computation for Smart Applications: The devices in IoT may not have the computational capacity to perform complex cryptographic calculations involved in the blockchain model. Since it is estimated that 50 billion devices will be connected to the internet by 2022, there should be enough devices online at any point of time, to perform these calculations.
- Information Exchange for Smart Applications: While it may be relatively easy to transfer the information and maintain a ledger for devices of the same type, IoT will have different types of devices and each device might store/process different kinds of information. Maintaining all this information in a single ledger might get complex and difficult to manage. Alternatives like sidechain can be utilized to solve this problem.
- Trusting the devices: More devices mean more risk. Each device might have different vulnerabilities and if they are exploited successfully by an attacker, it might lead to a complete takeover of the device. Blindly trusting all the devices in the blockchain might be a problem.

Table 1 lists the various difficulties in integrating blockchain technology with Internet of Things devices. Making sure every device is uniquely identified is one of the main challenges. To be tracked within the blockchain, each IoT device needs a unique identifier, which is usually accomplished using a pair of cryptographic keys (public and private). However, IP addresses are unreliable because they are dynamic, and many IoT devices, like lights or CCTV cameras, are unable to manage these keys. The problem of double spending, which is particularly pertinent to financial transactions, is another difficulty. Blockchain uses proof-of-work and mining techniques to address this problem. Even though double spending is not an issue for non-financial data transfers, a protocol for methodically adding blocks to the blockchain should still exist. Since many IoT devices lack the processing capacity to carry out the intricate cryptographic operations necessary for blockchain functionality, cryptographic computation presents another difficulty. Having enough devices that can manage these tasks is essential, given the quick rise in connected devices. IoT networks use a variety of devices that process various kinds of data in order to exchange information. It can become difficult to manage this data in a single blockchain ledger; sidechains are one way to improve management. Last but not least, trusting devices is a serious issue. Because every device has vulnerabilities, the risks rise as more are added to the network. A serious systemic breach could result from a compromised device. As a result, it is dangerous and may result in exploitation to blindly trust every device on the blockchain. To achieve safe and effective IoT and blockchain integration, these issues must be resolved.

IV. Implementation Challenges and Solutions for Blockchain-IoT Integration

Blockchain technology and the IoT have significant potential to revolutionize various industries, including supply chain management, smart cities, healthcare, and industrial automation. However, integrating blockchain into IoT ecosystems presents a number of complex operational, technical, and environmental issues. These challenges must be systematically resolved to guarantee the successful implementation of blockchain in IoT systems, particularly when considering the resource limitations and real-time processing demands specific to IoT devices. For instance, platform incompatibility often impedes seamless device integration, as different IoT devices and ecosystems may use proprietary protocols or data formats that are not inherently interoperable with standard blockchain frameworks. This fragmentation leads to complex middleware requirements and increases development overhead, slowing adoption. Furthermore, concerns about security and privacy are paramount. While blockchain offers strong cryptographic security, the sheer volume of IoT data and potential vulnerabilities at the device level remain a risk. A notable example is the Mirai botnet attack in 2016, which leveraged insecure IoT devices to launch massive distributed denial-of-service (DDoS) attacks, demonstrating how widespread device vulnerabilities can be exploited, even with robust network security in place. In order to facilitate successful implementation, this section examines the main obstacles to blockchain-IoT integration and provides workable solutions, which are covered in detail in the subsections that follow:

- A. Scaling and Network Latency: Significant scalability issues for blockchain systems have been brought about by the quick growth of IoT devices. Network latency is made worse by the requirement that every device take part in blockchain consensus procedures like Proof of Work (PoW) as the number of connected devices rises. For real-time applications, where prompt and effective data exchange is essential, this latency is especially troublesome. For example, latency in data transmission in healthcare systems can affect patient care and treatment results, while delays in processing sensor data in autonomous vehicles can endanger safety. PoW's energy-intensive nature also raises environmental concerns, which makes it less appropriate for widespread use in IoT networks where a large number of devices need continuous processing and validation. Many different strategies have been put forth to address the latency and scalability problems that blockchain systems in IoT applications present. While preserving the blockchain's security and integrity, these solutions seek to maximize transaction throughput and reduce latency as follows [43], [44]:
- Lightweight Consensus Algorithms: Delegated Proof of Stake (DPoS) and Proof of Stake (PoS) are good substitutes for Proof of Work (PoW), which greatly lowers the energy and computational load. These algorithms are better suited for the resource-constrained environments typical of IoT networks because they require fewer validators to reach consensus, which lowers the energy footprint and speeds up transaction validation.
- Layer 2 Solutions: To manage high-throughput transactions outside of the main blockchain network, technologies like sidechains and off-chain transactions have been developed. These solutions ease the strain on the primary blockchain by shifting some of the transaction processing to secondary layers, which speeds up processing and lowers latency. This makes it possible for

IoT applications to function more effectively in settings like industrial monitoring and autonomous systems that demand real-time data exchange.

- Sharding: Is the process of dividing the blockchain into more manageable, smaller sections, or "shards," each of which is able to process its smart contracts and transactions on its own. By dividing the processing and storage burden among several nodes, this method improves scalability and raises the blockchain network's overall performance. For applications that need high-frequency, low-latency interactions, sharding also helps to guarantee that transaction processing times are kept to a minimum.
- Private Blockchain Networks: Hyperledger Fabric and other permissioned blockchain networks can offer an environment for Internet of Things applications that is more efficient and controlled. Consensus mechanisms like Raft, which are less resource-intensive than PoW and can be customized to match the unique requirements of IoT systems, are used in these networks. The potential of Hyperledger Fabric for real-time Internet of Things applications was highlighted by a study that showed it could process up to 230.2 transactions per second (TPS) with a latency of 259.3 milliseconds.

Table 1. Challenges in Blockchain-IoT Integration for smart applications

Challenge	Description	Solutions/Considerations
Unique Identification for Smart Applications	Each IoT device requires a unique identifier for tracking within the blockchain. Many devices lack the capacity to manage cryptographic keys.	Use of public and private keys for device identification. IP addresses are unreliable due to their dynamic nature.
Double Spending Issue	Double spending must be prevented in blockchain for transactions involving monetary assets. Non-financial data transfers don't require prevention.	Mining and proof-of-work for monetary transactions. Protocols to build and append blocks for non-financial data.
Cryptographic Computation for Smart Applications	Many IoT devices lack the computational power to perform complex cryptographic operations required for blockchain.	Ensure sufficient devices online to perform the cryptographic computations. Need scalable devices for handling this.
Information Exchange for Smart Applications	IoT networks involve diverse devices storing and processing different types of data, making ledger management complex.	Use of sidechains to manage data from different devices effectively, easing ledger complexity.
Trusting the Devices	Each device has unique vulnerabilities, and compromising a device can lead to security breaches. Blind trust in devices is risky.	Carefully manage device trustworthiness. Risk management protocols to ensure secure interactions.

Fig. 4 shows how different consensus algorithms used in blockchain-IoT integration trade off latency and scalability. It demonstrates how private blockchain networks, sharding, Layer 2 solutions, and lightweight consensus mechanisms synergistically improve blockchain system performance in IoT environments, enabling the scalability needed for large-scale, real-time applications.

A. *Energy Efficiency in IoT Devices*

The power limitations of many IoT devices presents a major obstacle. The battery life of such devices can be rapidly depleted by running energy-intensive blockchain consensus mechanisms, especially Proof of Work (PoW). When IoT devices are placed in difficult-to-reach or remote areas, frequently without convenient access to power sources, this becomes particularly problematic. In order to ensure the long-term, sustainable operation of these devices without sacrificing the functionality of the underlying Internet of Things applications, energy efficiency becomes crucial. Innovative solutions that improve the overall energy efficiency of blockchain-IoT integration are required to balance the energy demands of blockchain operations with the operational requirements of IoT devices. Using edge computing is one promising way to address energy inefficiency in IoT devices. The computational load on resource-constrained IoT devices can be greatly decreased by shifting complex cryptographic operations to more competent edge nodes. This method optimises bandwidth and lowers energy consumption by ensuring that only the most pertinent data is sent to the blockchain network, in addition to helping to protect the energy of individual devices. Energy efficiency can also be increased by implementing lightweight consensus techniques like Proof of Stake (PoS) or Proof of Authority (PoA). PoS and PoA use a lot less energy to maintain consensus than PoW, which needs a lot of computing power and energy for transaction validation. They are therefore more appropriate for Internet of Things settings where power efficiency is a major consideration. Fig. 5 shows how edge computing lowers the overall energy demand of blockchain transactions in IoT applications by shifting energy-intensive tasks from IoT devices to more potent edge nodes. To further optimise energy consumption and ensure that the blockchain network maintains its efficiency while taking into account the power constraints of IoT devices, lightweight consensus protocols like PoS or PoA are integrated [45].

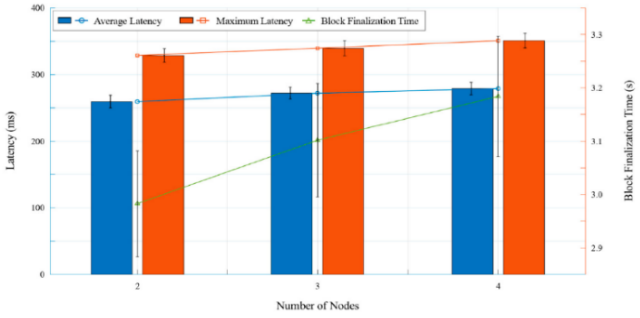

Fig. 4. Scalability and latency trade-offs between consensus algorithms in blockchain-IoT integration

B. *Data Integrity and Privacy*

Particularly in industries like healthcare, finance, and smart homes, the explosive growth of IoT devices has resulted in the creation of previously unheard-of amounts of private and sensitive data. Large amounts of extremely

sensitive data, including financial transactions, location data, and personal health information, are gathered, processed, and transmitted by these devices. With its intrinsic transparency and immutability, blockchain technology has a lot to offer in terms of protecting data integrity. But this openness may unintentionally reveal private information, raising serious privacy issues. For example, the blockchain makes sure that data records are verifiable and tamper-proof, but it does so in a way that makes the data accessible to all network users. This presents a problem, especially when handling private or sensitive data. As a result, protecting data integrity while preserving privacy becomes crucial. Privacy-preserving mechanisms must be integrated to ensure compliance and safeguard individuals' rights in industries like healthcare and finance, where privacy is subject to stringent regulatory frameworks (e.g., GDPR in the EU or HIPAA in the U.S.). Several cutting-edge cryptographic techniques can be used to address these privacy issues while maintaining the integrity of data stored on the blockchain. Homomorphic encryption is one such method that makes it possible to perform calculations on encrypted data without first decrypting it. This protects privacy while enabling the blockchain to verify the integrity of the data by guaranteeing that sensitive information is encrypted throughout its lifecycle. Using Zero-Knowledge Proofs (ZKPs), which enable the authenticity of a piece of data to be confirmed without disclosing the data itself, is another promising strategy. Without disclosing any private or sensitive information, ZKPs can be used to verify that a transaction is authentic or that data has not been tampered with. Because of this, ZKPs are the perfect way to preserve privacy in blockchain-based Internet of Things applications. An extra degree of security and privacy may also be offered by the use of permissioned ledgers or private blockchains.

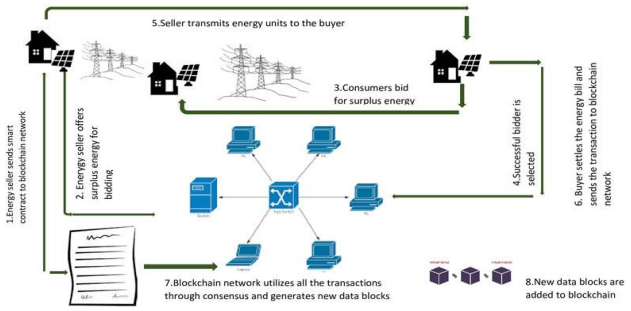

Fig. 5. Energy-efficient blockchain-IoT integration via edge computing

Private blockchains limit access to only those who are authorised, in contrast to public blockchains, which allow anyone to join the network. This makes it possible to have more control over who can access and validate transactions, guaranteeing that only trusted entities can see sensitive IoT data. A more fine-grained degree of control over data access and validation is made possible by permissioned blockchains, which further refine this by giving various users distinct roles and permissions. When combined, these tactics provide a strong framework for guaranteeing IoT system privacy and data integrity. Fig. 6 shows how IoT data privacy is ensured by integrating Zero-Knowledge Proofs into a blockchain network. The blockchain maintains its function as a safe and unchangeable record-keeping system while maintaining privacy by employing this cryptographic technique to authenticate transactions and confirm data integrity without disclosing the sensitive information that lies beneath [46].

C. *Interoperability Across IoT Devices*

Devices from various manufacturers that use various hardware configurations, communication protocols, and standards make up the naturally diverse Internet of Things (IoT) ecosystem. The smooth integration of IoT devices into a single system may be hampered by serious interoperability problems brought on by this diversity. Blockchain technology presents difficulties when implemented in diverse IoT environments, even though it has the potential to offer security, transparency, and immutability. These difficulties result from devices' incapacity to interact with one another across various protocols, which makes it difficult to create a coherent network and causes inefficiencies. Blockchain-based IoT systems may not operate at their best if interoperability problems are not fixed, which would restrict their scalability and practicality in fields like smart cities, healthcare, and industrial automation. Furthermore, the absence of a standardised method may make it difficult for blockchain solutions to be widely adopted since developers and manufacturers might be hesitant to embrace a system that necessitates a major reconfiguration of current infrastructure or devices [47].

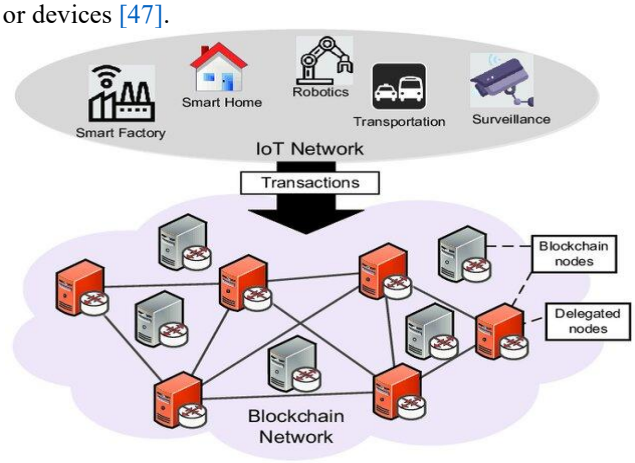

Fig. 6. Blockchain with zero-knowledge proofs for IoT data privacy

Several tactics must be used to get past the interoperability issues in IoT ecosystems. The creation and acceptance of standardised interoperability frameworks and Application Programming Interfaces (APIs) is one essential strategy. Blockchain can serve as a universal communication layer that connects devices from various manufacturers and technological capabilities by creating a common set of protocols, interfaces, and data formats. Regardless of the underlying software or hardware protocols, standardised APIs guarantee that a variety of IoT devices can securely and efficiently communicate with the blockchain, facilitating transactions and data exchange. Apart from standardised APIs, cross-chain interoperability solutions present encouraging developments. These solutions make it easier for various blockchain networks to communicate with one another, which is especially helpful when working with a wide range of IoT devices that might be installed on different blockchain platforms. The use of sidechains is one such technique that allows various IoT device types to function on distinct chains while preserving connectivity and data flow

with the main blockchain. This guarantees that specialised devices can function in their ideal settings and join a single blockchain network without sacrificing effectiveness or security. Furthermore, the limitation of device-specific protocols is removed by utilising blockchain-agnostic frameworks, which allow IoT devices to exchange data and communicate across various blockchain platforms. In IoT applications, these interoperability solutions improve blockchain's scalability and functionality. A more flexible and inclusive blockchain environment makes it simpler to add new devices to the network, which promotes wider adoption of blockchain solutions in a variety of IoT domains. Interoperability also makes it possible for devices to function independently while preserving safe, real-time data exchange, which is essential for Internet of Things systems that need to function with minimal latency, like industrial control systems or driverless cars. Fig. 7 illustrates the multitude of interoperability solutions that facilitate smooth communication and data exchange between diverse IoT devices within a blockchain framework, including standardised APIs, cross-chain interactions, and sidechains. The figure would show how blockchain can act as a universal layer of communication that guarantees the security, scalability, and efficiency of IoT systems by showing how these solutions integrate various IoT devices with the blockchain [48].

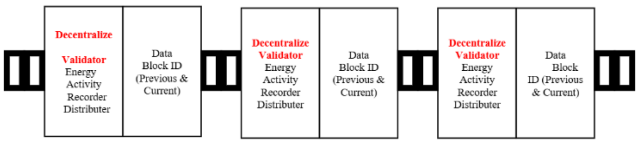

Fig. 7. Blockchain interoperability solutions for heterogeneous IoT devices

There are several important obstacles to overcome when integrating blockchain technology with the IoT, and each one calls for thoughtful analysis and specialised solutions to be implemented successfully. Because blockchain networks may be strained by the increasing number of IoT devices and their requirement for real-time communication, scalability and network latency are important issues. Layer 2 solutions like sidechains and sharding, in addition to lightweight consensus algorithms like PoS and DPoS, can be used to improve scalability and lower latency. Energy efficiency is also essential, particularly because a lot of IoT devices have limited resources. The energy requirements of blockchain operations can be reduced by using edge computing to offload intricate calculations and lightweight consensus techniques. Interoperability between various IoT devices running different protocols presents another difficulty. To ensure smooth communication and integration across heterogeneous systems, standardised APIs, cross-chain interoperability solutions, and blockchain-agnostic frameworks can aid in bridging these gaps. Lastly, legal and regulatory compliance are important factors to take into account, especially when handling sensitive data in Internet of Things applications. Blockchain's transparency and immutability provide a strong solution for keeping auditable records and guaranteeing data integrity, while smart contracts can be used to automate adherence to privacy laws and legal requirements. Table 2 provides a summary of these issues and suggested fixes [49].

V. Platform Considerations for Implementation and Simulation

The key performance metrics like latency, throughput, energy consumption, and transaction verification time must be taken into account when assessing which platforms are best suited for implementing the suggested blockchain-based IoT framework. Based on fictitious performance data, Fig. 8 compares four popular platforms: MATLAB, NS-3, Ethereum testnets, and hardware environments based on Raspberry Pi. Because of their versatility and large library, simulation tools like MATLAB and NS-3 are frequently used to model network protocols and communication in Internet of Things systems [50], [51]. Realistic blockchain transaction environments are provided by Ethereum testnets like Goerli and Rinkeby, which can highlight throughput and consensus time limitations [52].

Table 2. Implementation challenges and solutions for Blockchain-IoT integration

Challenge	Description	Solutions/Considerations
Scalability and Network Latency	Discusses the scalability challenges and latency issues related to blockchain networks in IoT systems, and proposes solutions like lightweight consensus algorithms, Layer 2 solutions, and sharding.	Use of lightweight consensus algorithms (PoS, DPoS), Layer 2 solutions (sidechains), and sharding to handle scalability and reduce latency.
Energy Efficiency in IoT Devices	Explores the energy efficiency challenges of blockchain-IoT integration, particularly in resource-constrained devices, and suggests solutions such as edge computing and lightweight consensus mechanisms.	Implement edge computing to offload complex computations from IoT devices, and use lightweight consensus protocols like PoS.
Interoperability Across IoT Devices	Highlights interoperability issues in heterogeneous IoT environments and proposes solutions such as standardized APIs, cross-chain interoperability, and blockchain-agnostic frameworks.	Adopt standardized APIs, cross-chain interoperability, and blockchain-agnostic frameworks to ensure seamless communication between diverse IoT devices.
Regulatory Compliance and Legal Issues	Addresses the regulatory compliance challenges in integrating blockchain with IoT systems, focusing on data privacy, legal requirements, and the use of smart contracts for automated compliance.	Incorporate smart contracts for automated compliance with data privacy laws and regulatory requirements, and use blockchain for transparent audit trails.

Real-world deployment problems, especially those pertaining to energy consumption and computational overhead, can be better understood through hardware-based prototyping with gadgets like Raspberry Pi [53]. This comparison helps future researchers choose the best platform

for validating secure IoT systems by highlighting the trade-offs between hardware limitations, blockchain realism, and simulation accuracy.

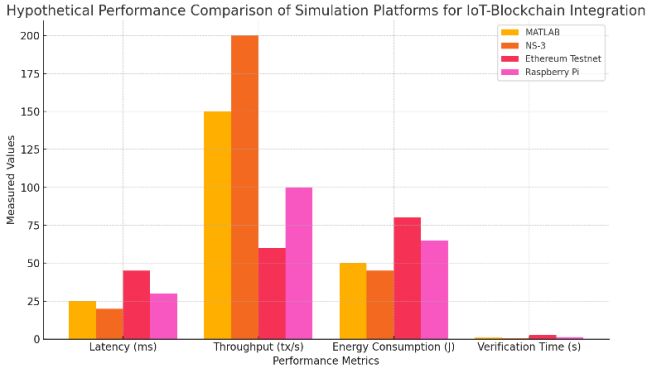

Fig. 8. Performance comparison of IoT–Blockchain platforms

VI. CONCLUSION

This paper shows that blockchain technology, especially Ethereum's proof-of-stake consensus mechanism, has a lot of potential for integrating IoT devices into applications for smart cities. In contrast to other platforms like Litecoin, Ethereum's well-established infrastructure provides significant benefits in terms of security, decentralisation, and scalability. In order to solve important issues with data privacy, device identity management, and secure data transfer within IoT networks, blockchain offers an environment for IoT data that is safe, transparent, and unchangeable. Blockchain is not a one-size-fits-all solution, despite its enormous potential. While blockchain is ideally suited for applications where security and decentralisation are critical, the paper emphasises that its implementation necessitates careful consideration of the resource limitations and operational requirements unique to Internet of Things devices. Furthermore, there are still problems that need to be resolved, such as scalability issues, energy efficiency issues, and the requirement for interoperability across heterogeneous IoT devices. Consequently, even though blockchain's integration with IoT ecosystems presents revolutionary opportunities, more study and technical developments are required to maximise its use and guarantee its widespread adoption in a variety of IoT contexts.

REFERENCES

[1] J. Akram, A. Akram, V. Sharma, A. Anaissi, R. H. Jhaveri and P. Verma, "Blockchain-Based Model for Secure and Fair Data Provision in Crowdsourced Drone Services," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 5221-5234, 2025, https://doi.org/10.1109/OJCOMS.2025.3575463.

[2] A. A. Sen, N. M. Bahbouh, S. Sendra, and O. Tayan, "PoPR: A Novel Blockchain Consensus Mechanism for Reliable Crowdsourced Data," *International Journal of Information Technology*, pp. 1-13, 2025, https://doi.org/10.1007/s41870-025-02547-4.

[3] N. Basil, H. M. Marhoon, D. F. Sahib, A. F. Mohammed, H. M. Ridha, and A. Ma'arif, "Accelerated Black Hole Optimization Algorithm with Enhanced FOPID Controller for Omni-Wheel Drive Mobile Robot System," *Neural Computing and Applications*, pp. 1-32, 2025, https://doi.org/10.1007/s00521-025-11310-6.

[4] S. Balasubramanian, R. Cyriac, S. R. A. Samad, R. Karthikeyan, and V. Balamurugan, "Optimized Memory-Augmented Deep Unfolding Network with Blockchain-Based Data Preserving Cyber Security in Internet of Things," *Knowledge-Based Systems*, vol. 321, p. 113536, 2025, https://doi.org/10.1016/j.knosys.2025.113536.

[5] F. Ellouze, G. Fersi, and M. Jmaiel, "Lightweight blockchain-based access control with efficient revocation for fog-enabled IoT," *Innovative Systems and Software Engineering*, vol. 21, no. 2, pp. 355-379, 2025, https://doi.org/10.1007/s11334-025-00608-2.

[6] V. Maurya *et al*., "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, p. 53, 2025, https://doi.org/10.1007/s12083-024-01812-w.

[7] N. Basil *et al*., "Multi-criteria decision model for multicircular flight control of unmanned aerial vehicles through a hybrid approach," *Scientific Reports*, vol. 15, no. 1, pp. 1-31, 2025, https://doi.org/10.1038/s41598-025-01508-y.

[8] H. M. Marhoon, A. I. Alanssari, and N. Basil, "Design and Implementation of an Intelligent Safety and Security System for Vehicles Based on GSM Communication and IoT Network for Real-Time Tracking," *Journal of Robotics and Control*, vol. 4, no. 5, pp. 708–718, 2023, https://doi.org/10.18196/jrc.v4i5.19652.

[9] A. Syed Muhammad Ali, S. Ali, K. Ziaullah, M. -I. Joo and H. -C. Kim, "IoMT and Blockchain Synergy: A Novel Approach to Health Data Validation and Storage," *IEEE Access*, vol. 13, pp. 57753-57766, 2025, https://doi.org/10.1109/ACCESS.2025.3555289.

[10] A. Shamaseen, M. Qatawneh, and B. Elshqeirat, "Smart Grid System Based on Blockchain Technology for Enhancing Trust and Preventing Counterfeiting Issues," *Energies*, vol. 18, no. 13, p. 3523, 2025, https://doi.org/10.3390/en18133523.

[11] N. Basil *et al*., "Performance analysis of hybrid optimization approach for UAV path planning control using FOPID-TID controller and HAOAROA algorithm," *Scientific Reports*, vol. 15, no. 1, p. 4840, 2025, https://doi.org/10.1038/s41598-025-86803-4.

[12] J. Alotaibi, "A hybrid software-defined networking approach for enhancing IoT cybersecurity with deep learning and blockchain in smart cities," *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, p. 123, 2025, https://doi.org/10.1007/s12083-025-01935-8.

[13] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang and K. Wu, "A Blockchain-Enabled AI-Driven Secure Searchable Encryption Framework for Medical IoT Systems," *IEEE Journal of Biomedical and Health Informatics*, 2025, https://doi.org/10.1109/JBHI.2025.3538623.

[14] N. Basil, H. M. Marhoon, and A. F. Mohammed, "Evaluation of a 3-DOF helicopter dynamic control model using FOPID controller-based three optimization algorithms," *International Journal of Information Technology*, pp. 1-10, 2024, https://doi.org/10.1007/s41870-024-02373-0.

[15] A. R. Ibrahim, N. Basil, and M. I. Mahdi, "Implementation enhancement of AVR control system within optimization techniques," *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 2021-2027, 2021, https://doi.org/10.22075/ijnaa.2021.5339.

[16] N. Basil, B. M. Sabbar, H. M. Marhoon, A. F. Mohammed, and A. Ma'arif, "Systematic review of unmanned aerial vehicles control: Challenges, solutions, and meta-heuristic optimization," *International Journal of Robotics and Control Systems*, vol. 4, no. 4, pp. 1794-1818, 2024, https://doi.org/10.31763/ijrcs.v4i4.1596.

[17] M. S. Al-Samarraay *et al*., "A new extension of FDOSM based on Pythagorean fuzzy environment for evaluating and benchmarking sign language recognition systems," *Neural Computing and Applications*, vol. 34, pp. 4937-4955, 2022, https://doi.org/10.1007/s00521-021-06683-3.

[18] I. M. Sharaf, O. S. Albahri, M. A. Alsalem, A. H. Alamoodi, and A. S. Albahri, "A novel dual-level multi-source information fusion approach for multicriteria decision making applications," *Applied Intelligence*, vol. 54, pp. 11577–11602, 2024, https://doi.org/10.1007/s10489-024-05624-6.

[19] A. M. A. Daiyan Kaif, K. Shahjahan Alam, S. K. Das, G. Chen, S. Islam and S. M. Muyeen, "Blockchain-Integrated Cyber-Physical Smart Meter Design and Implementation for Secured Energy Trading in Virtual Power Plants," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 15083-15093, 2025, https://doi.org/10.1109/TASE.2025.3566938.

[20] I. A. Reshi and S. Sholla, "IBF network: Enhancing network privacy with IoT, blockchain, and fog computing on different consensus mechanisms," *Cluster Computing*, vol. 28, no. 3, p. 208, 2025, https://doi.org/10.1007/s10586-024-05026-w.

[21] R. K. Munaganuri, N. R. Yamarthi, and S. C. Bolem, "Design of an improved graph-based model integrating LSTM, LoRaWAN, and blockchain for smart agriculture," *PeerJ Computer Science*, vol. 11, p. e2896, 2025, https://doi.org/10.7717/peerj-cs.2896.

[22] N. Basil and H. M. Marhoon, "Correction to: selection and evaluation of FOPID criteria for the X-15 adaptive flight control system (AFCS) via Lyapunov candidates: Optimizing trade-offs and critical values using optimization algorithms," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, vol. 8, p. 100589, 2024, https://doi.org/10.1016/j.prime.2024.100589.

[23] A. F. Mohammed, H. M. Marhoon, N. Basil, and A. Ma'arif, "A New Hybrid Intelligent Fractional Order Proportional Double Derivative+ Integral (FOPDD+ I) Controller with ANFIS Simulated on Automatic Voltage Regulator System," *International Journal of Robotics and Control Systems*, vol. 4, no. 2, pp. 463–479, 2024, https://doi.org/10.31763/ijrcs.v4i2.1336.

[24] A. F. Mohammed *et al*., "Selection and Evaluation of Robotic Arm based Conveyor Belts (RACBs) Motions: NARMA (L2)-FO (ANFIS) PD-I based Jaya Optimization Algorithm," *International Journal of Robotics and Control Systems*, vol. 4, no. 1, pp. 262–290, 2024, https://doi.org/10.31763/ijrcs.v4i1.1243.

[25] H. M. Marhoon, N. Basil, and A. Ma'arif, "Exploring Blockchain Data Analysis and Its Communications Architecture: Achievements, Challenges, and Future Directions: A Review Article.," *International Journal of Robotics and Control Systems*, vol. 3, no. 3, pp. 609–626, 2023, https://doi.org/10.31763/ijrcs.v3i3.1100.

[26] H. M. Marhoon, N. Basil, and A. F. Mohammed, "Medical Defense Nanorobots (MDNRs): a new evaluation and selection of controller criteria for improved disease diagnosis and patient safety using NARMA(L2)-FOP + D(ANFIS)μ–Iλ-based Archimedes Optimization Algorithm," *International Journal of Information Technology*, 2024, https://doi.org/10.1007/s41870-023-01724-7.

[27] M. Ghorbian and S. Ghorbian, "Blockchain and Machine Learning Integration with IoT for Healthcare Applications: A Novel Approach to Psoriasis Diagnosis," *Blockchain-Assisted Technologies for Sustainable Healthcare System*, Springer, pp. 67–86, 2025, https://doi.org/10.1007/978-981-96-3928-1_5.

[28] S. M. Rajagopal, M. Supriya, and R. Buyya, "Leveraging blockchain and federated learning in Edge-Fog-Cloud computing environments for intelligent decision-making with ECG data in IoT," *Journal of Network and Computer Applications*, vol. 233, p. 104037, 2025, https://doi.org/10.1016/j.jnca.2024.104037.

[29] M. T. Chaudhry, A. Yousafzai, A. Zia, S. A. Abid, and F. Ahmad, "Deadline-aware workload scheduling for edge-enhanced iot devices: A blockchain-enabled approach to incentive-based computing," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, p. 189, 2025, https://doi.org/10.1007/s12083-025-01992-z.

[30] N. B. Mohamadwasel, "Rider Optimization Algorithm implemented on the AVR Control System using MATLAB with FOPID," *IOP Conference Series: Materials Science and Engineering*, pp. 1-14, 2020, https://doi.org/10.1088/1757-899X/928/3/032017.

[31] B. Rathnayake, L. Gunathilake, R. Edirisinghe, and S. Perera, "EcoConstruct: a blockchain-based system for carbon trading in construction projects," *Construction Innovation*, vol. 25, no. 7, pp. 213–234, 2025, https://doi.org/10.1108/CI-08-2024-0224.

[32] N. Basil, H. M. Marhoon, M. R. Hayal, E. E. Elsayed, I. Nurhidayat, and M. A. Shah, "Black-hole optimisation algorithm with FOPID-based automation intelligence photovoltaic system for voltage and power issues," *Australian Journal of Electrical and Electronics Engineering*, vol. 21, no. 2, pp. 115–127, 2024, https://doi.org/10.1080/1448837X.2024.2308415.

[33] N. Basil and H. M. Marhoon, "Selection and evaluation of FOPID criteria for the X-15 adaptive flight control system (AFCS) via Lyapunov candidates: Optimizing trade-offs and critical values using optimization algorithms," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, vol. 6, p. 100305, 2023, https://doi.org/10.1016/j.prime.2023.100305.

[34] N. Basil, M. E. Alqaysi, M. Deveci, A. S. Albahri, O. S. Albahri, and A. H. Alamoodi, "Evaluation of autonomous underwater vehicle motion trajectory optimization algorithms," *Knowledge-Based Systems*, vol. 276, p. 110722, 2023, https://doi.org/10.1016/j.knosys.2023.110722.

[35] N. Basil and H. M. Marhoon, "Towards evaluation of the PID criteria-based UAVs observation and tracking head within resizable selection by COA algorithm," *Results in Control and Optimization*, vol. 12, p. 100279, 2023, https://doi.org/10.1016/j.rico.2023.100279.

[36] G. Wang, Z. Shi, M. Nixon and S. Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage," *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 166-175, 2019, https://doi.org/10.1109/Blockchain.2019.00030.

[37] J. Huang, L. Kong, G. Chen, M. -Y. Wu, X. Liu and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680-3689, 2019, https://doi.org/10.1109/TII.2019.2903342.

[38] A. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques," *Mathematics*, vol. 11, no. 9, p. 2073, 2023, https://doi.org/10.3390/math11092073.

[39] N. B. Mohamadwasel and A. Ma'arif, "NB Theory with Bargaining Problem: A New Theory," *International Journal of Robotics and Control Systems*, vol. 2, no. 3, pp. 606-609, 2022, https://doi.org/10.31763/ijrcs.v2i3.798.

[40] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Scientific Reports*, vol. 14, no. 1, p. 7841, 2024, https://doi.org/10.1038/s41598-024-58578-7.

[41] Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1877-1890, 2021, https://doi.org/10.1109/JAS.2021.1004003.

[42] I. Masood, A. Daud, Y. Wang, A. Banjar, and R. Alharbey, "A blockchain-based system for patient data privacy and security," *Multimedia Tools and Applications*, vol. 83, no. 21, pp. 60443-60467, 2024, https://doi.org/10.1007/s11042-023-17941-y.

[43] Z. T. Al-Qaysi *et al*., "Optimal Time Window Selection in the Wavelet Signal Domain for Brain–Computer Interfaces in Wheelchair Steering Control," *Applied Data Science and Analysis*, vol. 2024, pp. 69-81, 2024, https://doi.org/10.58496/ADSA/2024/007.

[44] Z. T. Al-Qaysi *et al*., "A Frequency-Domain Pattern Recognition Model for Motor Imagery-Based Brain-Computer Interface," *Applied Data Science and Analysis*, vol. 2024, pp. 82–100, 2024, https://doi.org/10.58496/ADSA/2024/008.

[45] M. Elkhodr, S. Khan, and E. Gide, "A novel semantic IoT middleware for secure data management: Blockchain and AI-driven context awareness," *Future Internet*, vol. 16, no. 1, p. 22, 2024, https://doi.org/10.3390/fi16010022.

[46] I. Hussain, H. A. Hussain, N. Ullah and S. Misak, "A Novel Prosumer-Centric Smart Contract Based Approach for Blockchain-Enabled Energy Scheduling Using Electric Vehicles," *IEEE Access*, vol. 12, pp. 120747-120760, 2024, https://doi.org/10.1109/ACCESS.2024.3451186.

[47] D. Shah *et al*., "Blockchain factors in the design of smart-media for e-healthcare management," *Sensors*, vol. 24, no. 21, p. 6835, 2024, https://doi.org/10.3390/s24216835.

[48] M. Mulenga, K. O. Phiri, G. Mukupa, and A. Zimba, "Blockchain technology and energy efficiency: A systematic literature review of consensus mechanisms, architectural innovations, and sustainable solutions," *Research Square*, 2024, https://www.researchsquare.com/article/rs-6457924/v1.

[49] S. S. M. Abdul, "Navigating blockchain's twin challenges: Scalability and regulatory compliance," *Blockchains*, vol. 2, no. 3, pp. 265-298, 2024, https://doi.org/10.3390/blockchains2030013.

[50] E. K. Sari, A. Wirara, R. Harwahyu and R. F. Sari, "Lora Characteristics Analysis for IoT Application using NS3 Simulator," *2019 IEEE R10 Humanitarian Technology Conference (R10-HTC)(47129)*, pp. 205-210, 2019, https://doi.org/10.1109/R10-HTC47129.2019.9042485.

[51] P. Mishra, R. K. Patjoshi and A. K. Yadav, "A Delay Compensation Approach for IoT-Enabled Networks with Different Control Strategies," *2023 Fifth International Conference on Electrical,*

Computer and Communication Technologies (ICECCT), pp. 1-5, 2023, https://doi.org/10.1109/ICECCT56650.2023.10179610.

[52] S. B, A. S. Sh, S. K. E, S. N. K and N. S, "Blockchain Industry 5.0: Next Generation Smart Contract and Decentralized Application Platform," *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, pp. 1-8, 2022, https://doi.org/10.1109/ICSES55317.2022.9914151.

[53] I. Calvo, J. M. Gil-García, I. Recio, A. López, and J. Quesada, "Building IoT Applications with Raspberry Pi and Low Power IQRF Communication Modules," *Electronics*, vol. 5, no. 3, p. 54, 2016, https://doi.org/10.3390/electronics5030054.