IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 58, No. 9, September, 2025, pp. 1813-1821
Journal homepage: http://iieta.org/journals/jesa

Enhancing IoT Network Data Monetization with Blockchain: A Decentralized Approach Using Ethereum Blockchain Contract

Tariq Emad Ali[1*], Alwahab Dhulfiqar Zoltán[2]

[1] Information and Communication Engineering, Al-Khwarizmi College of Engineering, University of Baghdad, Baghdad 10070, Iraq
[2] Biomatics and Applied Artificial Intelligence Institution, John von Neumann Faculty of Informatics, Obuda University, Budapest 1034, Hungary

Corresponding Author Email: tariqemad@kecbu.uobaghdad.edu.iq

https://doi.org/10.18280/jesa.580904

Received: 1 January 2025
Revised: 7 February 2025
Accepted: 15 February 2025
Available online: 30 September 2025

Keywords:
DCAPP, IoT, BLCH, P2P, SaaS

ABSTRACT

Blockchain (BLCH) has emerged as a transformative technology for securing and decentralizing data transactions in the Internet of Things (IoT). By leveraging a distributed and incontrovertible record, BLCH enables trustless and transparent interactions among IoT nodes, ensuring security, traceability, and real-time verification. Given the diverse nature of IoT devices from sensors to actuators blockchain provides a robust framework for secure and decentralized data exchange, eliminating the need for centralized intermediaries. This paper explores the monetization of IoT network data using blockchain, proposing a decentralized application (DCAPP) built on the Ethereum blockchain. Our approach employs Blockchain Contracts BLCOs to facilitate secure and automated transactions in a Sensing-as-a-Service (SaaS) marketplace, where IoT sensor data can be bought and sold efficiently. By integrating blockchain, our model enhances data accessibility, trust, and scalability, addressing key challenges in security and interoperability. In this paper, we examine BLCH possible to redesign IoT systems, concrete the technique for safe and incentivized data-driven claims.

1. INTRODUCTION

Internet of Things (IoT) is growing quickly, determined by progresses in 5G expertise and its requests in smart homes, smart cities, e-health, and etc. But this development makes known to important safety and confidentiality challenges [1]. Given the decentralized landscape of IoT networks, traditional safety instruments are often unsuccessful in safeguarding protected announcement between IoT nodes. BLCH has developed as a capable key to develop safety in IoT communications [2]. It proposes a decentralized, distributed, and widely verifiable archive that securely archives communications between IoT devices. Data within the BLCH is accomplished alone over a peer-to-peer (P2P) network topology, confirming transparency and fixity [3]. In a BLCH-based IoT system, communications are verified as blocks, each cryptographically related to the earlier one. This construction allows visible and tamp unaffected statement crossways IoT nodes while keeping decentralized control [4]. The combination of BLCH and IoT within cloud settings is probable to develop IoT infrastructures, talking main challenges associated to safety, scalability, and confidence. The prime points of BLCH -IoT combination contain [5]:

(1) Decentralization: Individually BLCH and IoT logically survey a decentralized method, disregarding SPOF and refining structure flexibility.

(2) Safety: BLCH confirms protected statement among IoT devices by authenticating communications a cryptographically.

(3) Identification: Each IoT node and BLCH block has a single identifier, allowing reliable and confirmable information storing.

(4) Dependability: Communications in a BLCH network suffer confirmation by miners before being added to the chain, certifying statistics veracity.

(5) Independence: IoT nodes can interrelate straight in a BLCH network lacking trusting on centralized authorities.

(6) Scalability: BLCH enables immediate, high obtainability statement between IoT nodes in a scattered network.

Out there safeguarding IoT networks, BLCH similarly acting a vibrant part in maximizing the rate of IoT created statistics. As the number of installed sensors stays to raise, so does the want for effective data monetization policies. The Sensing-as-a-Service (SaaS) classical reports this task by permitting sensor holders to mint their data, as long as clients with continuous entree to immediate sensor analyses deprived of the requirement to keep physical sensors [6]. This paper grants a BLCH based decentralized SaaS application, considered to enable protected and translucent sensor data communications. The projected stand, made on the Ethereum BLCH, powers keen contracts to power and confirm transactions deprived of needing a vital expert. Ethereum was designated for its strength, safety, and fixed growth ecosystem,

construction it a perfect optimal for decentralized application (DCAPP). Ethereum offers a Turing whole setting for implementing BLCOs, permitting designers to shape safe and scalable DCAPP. Disparate traditional client-server constructions that depend on authorization exchange transactions over a vital object, Ethereum's BLCO instrument allows straight P2P transactions using cryptocurrency, attractive safety and transparency. To validate the proposed approach, a blockchain-based marketplace for IoT weather sensor data has been developed. This platform allows users to access and trade sensor data using a custom token designed specifically for this application. The Ethereum blockchain's flexibility, security, and widespread adoption make it the preferred platform over alternatives such as EOS, Cardano, Stellar, and NEO.

The rest of the paper is structured as follows: Section 2 reviews the literature on blockchain and IoT integration, Section 3 explores the role of blockchain in IoT security, Section 4 present the blockchain operation in IoT, Section 5 explores the system overview and requirements, Section 6 prototype implementation, Section 7 show the experimental results, and Section 8 present the privacy enhancing technologies for blockchain based IoT systems, Section 9 discusses the challenges, and Section 10 concludes the study.

2. LITERATURE REVIEW

Security and privacy in IoT communications have recently gained significant attention, with numerous studies exploring methods to secure data exchange among IoT devices. One of the earliest discussions on secure document exchange without storing timestamp information was presented by Aounzou et al. [7]. This foundational idea contributed to the later development of blockchain technology, which was formally introduced by Rathore et al. [8]. Building on these concepts, Khan et al. [9] introduced "IoTChain," a blockchain-based authentication framework designed to secure data exchange between IoT nodes. Additional revisions take discovered diverse manners to support IoT safety. For occurrence, the combination of fog and mobile ad hoc network (MANETs) for protected smart device statement was surveyed in the study [10], while the Net Fog basis planned in the study [11] designed to deliver a safe statement classical for IoT strategies. Middleware results easing safe data entree crossways fog MANET constructions were extra discovered in the study [12]. Furthermore, IoT node statement dependability was examined in the study [13], although investigate on flexibility representations for IoT infrastructures in 5G systems was directed in the study [14]. A fuzzy logic-based flexibility basis for safeguarding IoT infrastructures was also proposed in the study [15].

Further topical revisions take attentive on participating blockchain technology with IoT to enhance security, privacy, and data management. Raouf [16] investigated how BLCH can decentralize IoT data ownership and control, educating safety and effectiveness while talking challenges, such as scalability and data assortment. Likewise, Bordel Sánchez et al. [17] planned a BLCH-enabled market for impartial manufacturing data transaction via NFTs and IPFS. Their explanation safeguards confidentiality over data makes random and permits safe communications via NFT ownership, through investigational justification indicating developments in statistics communications and operator involvement for manufacturing negotiators. Zhou et al. [18] led an inclusive examination on participating zero-knowledge proofs (ZKP) into BLCH based individuality distribution organizations. They examined progressions, challenges, and prospects whereas providing commendations grounded on practical circumstance revisions and exactness upcoming investigation instructions. Additional examination by Shafik [19] inspected the meeting of BLCH and IoT, investigating its prospects, challenges, and probable explanations. Their study recognized investigate holes, studied practical custom suitcases, and planned frameworks to address problems such as scalability, safety, and interoperability, providing visions to development BLCH and IoT implementation. Trivedi et al. [20] measured BLCH based IoT keys with a concentration on confidence, safety, and presentation challenges. They investigated low-power agreement procedures, BLCO strategy, and interoperability, giving an instance study on mining costs and latency. Their investigation emphasized BLCH IoT attacks, open matters, and future examine instructions for emerging safe and effective BLCH IoT ecosystems.

A complete examination on BLCH and IoT safety was shown in the study [21], importance the possible of BLCH in enhancing IoT claims. BLCH role in SaS was observed in the study [22], where main appearances of Bitcoi such as decentralization, pseudonymous ID, and cryptographic verifiability were leveraged to safe sensor data transactions. Ali et al. [23] projected connecting individually sensor to the Bitcoin BLCH, permitting operators to demand and pay for data using Bitcoin transactions. But, challenges such as data transparency and transaction scalability were recognized, which were far along talked over BLCOs. This allowance presented a useful prototype that used Ethereum BLCOs to proposal more give in sensor data admission while refining safety. The combination of BLCH technology into IoT device administration was extra discovered in the study [24], where Ethereum was used to construct IoT devices and safeguard data integrity. A practical experimentation concerning smartphones and Raspberry Pi based energy meters verified how Ethereum BLCOs can implement energy usage strategies. Though, the study emphasized restrictions such as measured transaction times (approximately 12 seconds) and the essential for large storing to maintain BLCH archives, which continued current challenges [25].

Although BLCH offerings a hopeful explanation for safeguarding IoT networks, numerous challenges keep on. Matters such as BLCH scalability, transaction costs, and data privacy worries were emphasized in the study [26]. Furthermore, BLCH transparency attitudes confidentiality challenges, as all transactions are publicly visible, construction private data defense intricate. Furthermore, miner selection remnants a serious subject, as miners can impact transaction justification, possibly chief to safety hazards. Despite these challenges, the merging of BLCH and IoT has the probable to transform productions by presenting decentralized confidence models and allowing new commercial opportunities.

3. ROLE OF BLCH IN IOT

IoT allows whole statement among consistent physical devices over diverse networks [27]. The IoT ecosystem is characteristically organized into four main mechanisms:

(1) Physical Nodes: Individually IoT node is allocated a single ID, permitting it to conversation statistics with other

associated nodes.

(2) Gateways: Substitute as mediators among IoT nodes and the fog, gateways confirm safe statement and constant network connectivity.

(3) Networking: This section accomplishes information stream and enhances routing routes to improve statement effectiveness.

(4) Fog Structure: Fog is in charge for storage and meting out the huge quantities of information caused by IoT nodes.

BLCH acting a vital character in safeguarding IoT infrastructures by providing a circulated, tamp unaffected archive for confirming and storage transactions. Different traditional centralized records, BLCH functions on a decentralized confidence model, enhancing safety and reducing confidence on a single authority. BLCH can be confidential into three categories public, private, and grouping respectively contribution diverse stages of entree control and transparency. A key division among BLCH based and traditional centralized records lies in their important possessions. Although centralized records depend on a single trusted object, often resulting in safety weaknesses and incomplete public access, BLCH suggestions a decentralized framework with high safety, transparent data access, and variable steps of privacy control. This makes BLCH a superior optimal for IoT applications that need safe, actual data connections. Numerous BLCH based stages are intended exactly to funding IoT applications [28]:

(1) IOTA: A next generation BLCH considered for high data integrity, effective transaction dispensation, and minimal reserve feeding, talking BLCH scalability restrictions.

(2) OTIFY: A web-based stand contribution convention IoT applications to mitigate BLCH limitations and improve interoperability.

(3) iExec: An open-source blockchain framework that integrates decentralized cloud computing for IoT applications.

(4) Xage: A safety intensive BLCH stage considered to improve computerization and safe data conversation in IoT settings.

(5) SONM: A decentralized fog computing stand leveraging BLCH knowledge to deliver safe fog-based services.

The merging of BLCH and IoT is driving new business chances and transforming industries by permitting actual, safe, and independent machine-to-machine (M2M) communications. This decentralized method not only safeguards data validity and confidentiality but also improves scheme resilience by dropping SPOF. BLCH technology can professionally track and organize billions of associated IoT nodes, facilitate safe transactions, and generate a more adaptive and stronger ecosystem. By leveraging cryptographic hashing techniques, BLCH reinforces data confidentiality, safeguarding that sensitive data remains protected while supportive the scalability requirements of recent IoT App.

4. OPPORTUNITIES

Mixing BLCH with IoT offerings an extensive variety of openings, solving novel potentials for both technologies. Some of the important advantages of this combination contain [29]:

(1) Founding Confidence Among Nodes: BLCH improves confidence in IoT networks by safeguarding that only authentic and confirmed nodes can link. Each transaction block suffers authentication by miners before being further to the BLCH, avoiding illegal entree.

(2) Cost Saving: By permitting straight statement among IoT nodes, BLCH removes the requirement for mediators, meaningfully dipping effective costs. Transactions happen P2P, cutting out third party service workers.

(3) Faster Transactions: Traditional transaction handing out can receipts hours or even days. With BLCH, the time vital for information connections and financial transactions is reduced to mere seconds.

(4) Improved Safety and Confidentiality: BLCH cryptographic instruments deliver strong safety for IoT networks, defensive nodes and information from meddling, unauthorized entree, and cyber threats.

(5) Upgraded Community Facilities: BLCH-IoT combination permits continuous statement and info conversation between associated nodes, pretty public and social services.

(6) Safe Economic Services: BLCH based IoT keys enable fast, safe, and remote economic transactions without the requirement for third-party mediators. This not only hurries up account transfers but also lowers costs.

(7) Risk Administration: By leveraging BLCH transparency and immutability, IoT structures can improved evaluate and mitigate dangers, dropping failures in reserve organization and transaction dispensation.

The interaction among BLCH and IoT is transforming industries by providing safe, efficient, and scalable keys. As this combination stays to develop, it will cover the method for a more associated and robust digital ecosystem.

5. SYSTEM OVERVIEW AND REQUIREMENTS

This paper offerings the advance of an Ethereum based DCAPP intended to simplify purchasing and marketing IoT device information over a BLCH market. Transactions are accepted out by means of a custom token called CustToken, which attends as the payment coins. For the determination of this investigate, we formed and experienced CustTokento discover Ethereum's abilities. The request is intended for IoT weather sensors, but with negligible adjustments, it can provision any other type of IoT sensor. The structure is composed of two key mechanisms:

```
contract CustToken {
    string public name = " CustToken";
    string public symbol = "Cust";
    uint8 public decimals = 18;
    uint256 public totalSupply = 900000000 * (10 **
uint256(decimals));

    mapping(address => uint256) public balanceOf;

    constructor() {
        balanceOf[msg.sender] = totalSupply;  // Assign all
tokens to the contract deployer
    }
    function transfer(address recipient, uint256 amount)
public returns (bool) {
        require(balanceOf[msg.sender] >= amount,
"Insufficient balance");
        balanceOf[msg.sender] -= amount;
        balanceOf[recipient] += amount;
        emit Transfer(msg.sender, recipient, amount);
        return true;
    }
    event Transfer(address indexed from, address indexed
to, uint256 value);
}
```

Figure 1. CustToken issuance clarification

A. Blockchain Contracts (BLCO): Two Ethereum BLCO govern the structure:

1. CustToken Contract: Creates and manages CustToken and its specifically developed for research and experimentation. The total supply of CustToken is fixed at 900,000,000 units as shown in Figure 1. This means that no more tokens will be minted after deployment, ensuring that the token is not inflationary. The token uses 18 decimal places, which is a standard for ERC-20 tokens. This allows for precise transactions.

2. Broker Contract: Broker contract, shown in Figure 2, is responsible for handling the registration of sensors, processing transactions, and managing data exchanges between buyers and sellers. Specifically, the buyData function performs the validation of transactions.

Figure 3 represents the buyData function's validation logic.

```
import "./ CustToken.sol";

contract Broker {
   CustToken public custToken;  // Reference to the
CustToken contract
   mapping(address => uint256) public dataPrices;  //
Price of data per sensor
   mapping(address => bool) public sensors;  //
Registered sensors

   constructor(address _ CustToken) {
      CustToken = CustToken (_CustToken);
   }

 // Register a new IoT sensor
   function registerSensor(address sensor, uint256 price)
public {
      sensors[sensor] = true;
      dataPrices[sensor] = price;
   }
   // Buy sensor data from the seller
   function buyData(address sensor) public {
      require(sensors[sensor], "Sensor is not registered");
      uint256 price = dataPrices[sensor];
      require(CustToken.balanceOf(msg.sender) >= price,
"Insufficient funds to buy data");
// Transfer CustToken from buyer to seller
      address seller = sensor;  // In this case, the sensor
itself is the seller
      CustToken.transferFrom(msg.sender, seller, price);

      // Log the transaction (for traceability)
      emit DataTransaction(msg.sender, seller, sensor,
price);
   }

   // Event to log the data transaction
   event DataTransaction(address indexed buyer, address
indexed seller, address indexed sensor, uint256 price);
}
```

Figure 2. Broker contract logic

B. Web Application: The web application acts as a user-friendly interface that enables seamless interaction with the blockchain. It allows users to:

- Browse and purchase sensor data.
- Send transactions to BLCOs.
- View and access purchased data.
- Prevent common transaction errors, such as mistyping Ethereum addresses, which could result in the loss of funds.

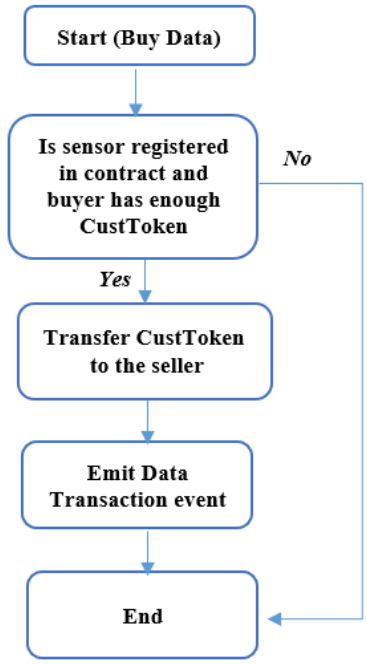

Figure 3. BuyData function's validation logic

C. User Categories: The system supports three distinct user roles:

- BLCO Owner: - It is the individual who deploys and manages the BLCOs, controls the price of CustToken in ether, and realizes its balance.
- IoT Sensor Workers: - The own Externally Owned Accounts (OEOA) and record their devices on the BLCH. He cannister modify their sensor information (e.g., data pricing), and provide sensor data via a RESTful API, earn CustToken from selling sensor data, and he can exchange CustToken for ether.
- Data Buyers: - The purchase IoT sensor data using CustToken. They can exchange ether for CustToken when needed and gain access to the data they have purchased.

D. Buying and Selling IoT Sensor Data: The process of registering a sensor and selling data follows these steps:

- A sensor operator accesses the web application and registers a new IoT sensor.
- A transaction is sent to the Broker Contract, including sensor details (e.g., type, location).
- The operator maintains a RESTful API that serves sensor data upon request.
- Once registered, sensor data is stored on the blockchain and becomes available for purchase.

The buying process includes:

- The buyer visits the web application and browses available sensors.
- After selecting a sensor, they choose a time range for data access.
- The buyer initiates a blockchain transaction to purchase the data.
- If the buyer has enough CustToken, the transaction is successful:

  - The sensor operator receives CustToken.
  - The buyer gains access to the purchased data.
- If the buyer lacks sufficient tokens, the transaction fails they can purchase more CustToken using ether.

E. Token Transactions and Pricing

• Sensor operators receive CustToken for selling data.

• They can hold onto the tokens or sell them back for ether.

• The default exchange rate is 1 CustToken= 1 Ether, but the BLCO owner can adjust this price.

• The CustToken contract stores ether collected from token sales.

• The contract owner can withdraw ether from the contract balance or deposit additional ether if needed.

6. PROTOTYPE IMPLEMENTATION

BLCH-enabled IoT data framework shown in Figure 4 illustrates the integrates IoT devices, a web application, BLCOs on a blockchain, and MariaDB to enable secure and transparent IoT data transactions.

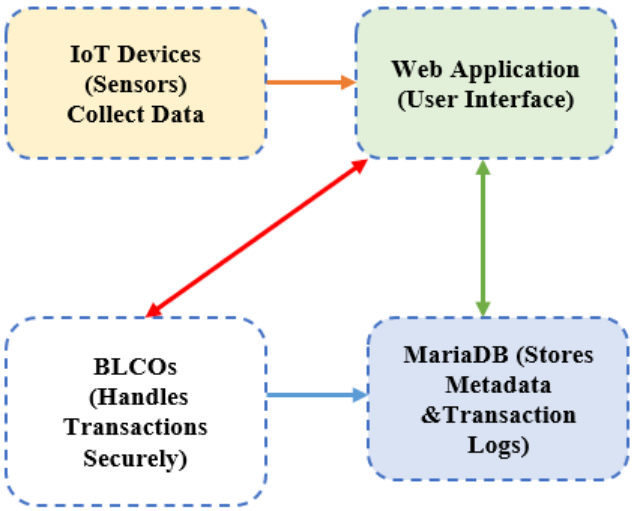

Figure 4. Blockchain-enabled IoT data framework

6.1 BLCOs

Once deployed to the BLCH, the code of BLCOs becomes immutable, which means it cannot be changed. Therefore, throughout the progress of the BLCOs, further maintenance was occupied throughout the taxing phase to ensure that as many bugs as possible were identified and fixed. The development of these contracts was carried out using the "Remix" web-based IDE. One of the key challenges addressed during the implementation was optimizing the code to minimize the gas costs associated with each function call. This optimization ensures that the transaction fees, which are paid when interacting with the BLCOs, are kept as low as possible.

(1) CustToken: It's a BLCO creates a custom token called Cust. CustToken have eighteen-unit places. The token's symbol is CustToken. The contract includes several key functions. One such function is the fallback function, which allows users to send Ether to the contract in exchange for CustToken. There's also a sell Back function that enables users to sell their CustToken return to the agreement and accept Ether in reappearance. The contract owner has special privileges, such as the ability to modification the charge of a CustToken and recover from the equilibrium. For token transfers between accounts, the contract implements three functions:

• A private function that transfers CustToken between accounts.

• A public function that calls the _transfer function to facilitate external transfers.

• BrokerTransferFrom: This function is invoked by the Broker contract to transfer CustToken at purchase IoT device information.

(2) Broker: It's a BLCO tracks all registered IoT sensors and enables sensor owners to update evidence concerning their devices. It also switches and archives transactions associated to the buying of IoT elements sensor statistics. The contract uses binary structs to store information about the sensors and the transactions. For each sensor, the contract stores details such as the owner, sensor type, price per measurement, first measurement time, frequency, location, and the URL somewhere the information is accessible. A key function within the Broker contract is createSensor, which allows sensor owners to register their sensors within the application. The contract emits a SensorCreated event upon successful registration. Additionally, functions like (change Sensor Seller, change Sensor Price, and change Sensor URL) allow sensor owners to modify their sensor's information. These functions emit events to notify the network whenever changes are made. The buyData function allows users to purchase sensor information for a definite interlude. Upon successful payment, the transaction is completed and an incident called TransactionDone is produced, granting the customer entree to the information.

6.2 Website and database

The website serves as the user interface for interacting with the blockchain, enabling users to view information and perform transactions quickly and easily. The website is compatible with Ethereum-based browsers allowing users to send transactions to the BLCH directly from their browser. The flow website shown in Figure 5 is built using "Node-RED", a stream built advance instrument constructed on top of "Node.js". The backend uses "JavaScript", while the front-end is developed with HTML, jQuery, and Bootstrap. The Node.js server continuously monitors the BLCH for actions from the BLCOs. When an incident is spotted, a record is kept in a MariaDB record, which is used to improve performance. Although all material is kept in the BLCH, retrieving data from a relational database (like MariaDB) is faster than querying the blockchain directly. This speeds up response times without affecting the decentralized nature of the application. The website offers several key functionalities, including:

(1) Viewing all user purchases and selecting individual purchases to view corresponding data.

(2) Searching and filtering available sensors.

(3) Viewing details about a sensor and purchasing data from it.

(4) Managing CustTokenbalances.

(5) Registering new sensors or changing sensor details.

(6) Viewing transaction histories related to the BLCOs.

(7) Managing the Ether balance and CustTokenprice.

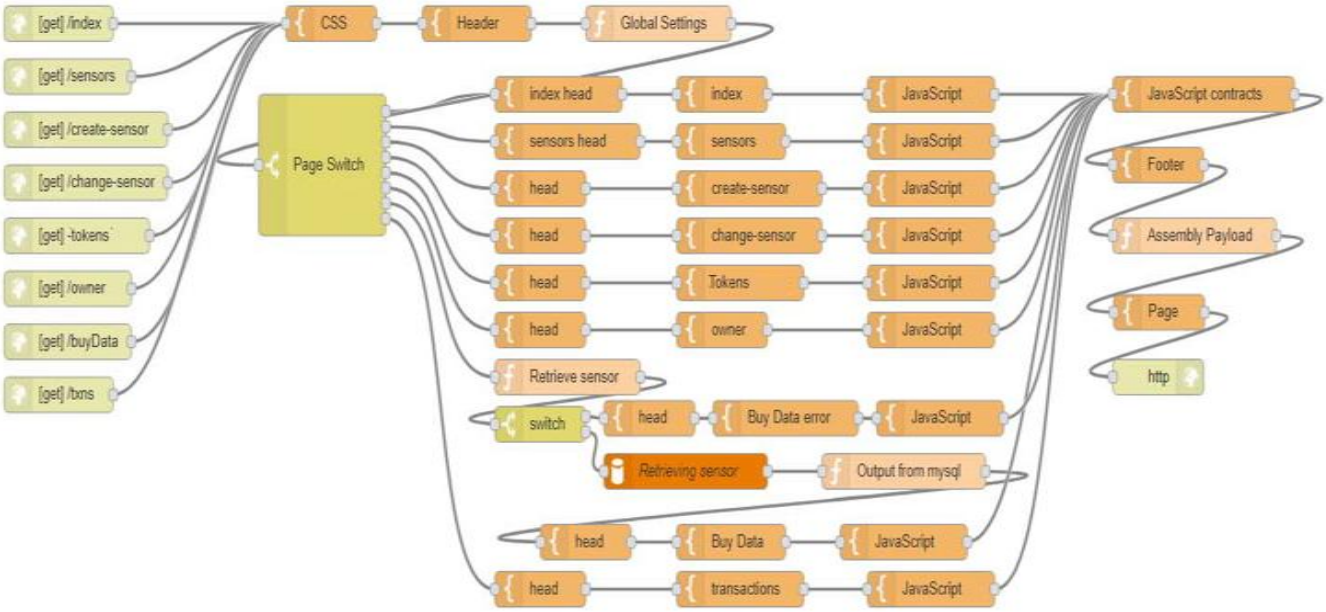

Figure 5. Flow designed for HTTP requests

6.3 Data sources

During the development phase, IoT weather sensor data was simulated using an API from Dark Sky. Node-RED flows were used to request real-time weather data, including parameters like air temperature, stickiness, compression, visibility, wind speed, and UV radiation, from various locations. These data were then stored in a MariaDB database. The application showing an application programing interface to assist the sensor information to handlers once demanded. When a user requests data, the system verifies their identity through a signed message. If the user has purchased data from a specific sensor, the system retrieves the necessary data using the sensor operator's API key, then serves it to the user. This method of managing data ensures that data transactions between buyers and sensor operators are secure and efficient while maintaining the decentralized nature of the application.

7. EXPERIMENTAL RESULTS

After deploying the BLCOs to the "Ropsten" Test Net, we measured the gas consumption for each noninternal purpose and assessed the interruption in operation confirmations. The gas fees for executing each function can be calculated using the Eq. (1).

$$Fee = gas\ used * gas\ price \quad (1)$$

where, the gas price in Wei, and 1 Wei = 10-18 ether. To illustrate, we assumed a gas price of 18500000000 Wei on January 15. This value allows us to compute the transaction fee in USD for each function, as shown in Table 1. It is important to note that the gas usage for functions remains constant regardless of the number of sensors stored on the blockchain or the age of the block containing the sensor data. Moreover, this usage is unaffected by whether the BLCO is installed on the Ethereum Mainnet, the Ropsten Testnet, or even a private network. However, transaction approval delays showed some variability. On the Ropsten Testnet, the delay ranged from just a few milliseconds to a maximum of 1 minutes. This delay depends on several factors, including the network's current state and cost and etc. The capability is projected to rise from 15 to 1 million.

Table 1. Amount paid for each function's execution (fixed price)

Function	Gas Usage
CustToken _constructor	0.018470147
Reserve role (billed)	0.00064695 – 0.00093736
ChangeCharge	0.000497568 – 0.000505798
RecoverEthereum	0.000550062 – 0.000557318
Transmission	0.000675019 – 0.000966702
Broker_constructor	0.01869694
GenerateSensor	0.002469219 – 0.002472786
AlterationSensorSupplier	0.000515092 – 0.000516289
AlterationSensorCharge	0.000491436 – 0.000512385
buyData	0.002096952

Table 2. Performance comparison: Optimized blockchain vs. Aws IoT for IoT data transactions

Metric	Optimized Blockchain	AWS IoT (Centralized System)
Transaction Cost (per transaction)	$0.0001 – $0.01	$0.0005 – $0.002
Transaction Speed (sec)	0.3-1	0.7-1.3
Security	High – Cryptographically secured, tamper-proof transactions	Medium – Centralized, vulnerable to hacking and data breaches
Decentralization	Fully decentralized, no single point of failure	Fully centralized, dependent on AWS servers
Data Ownership	Users fully control their data	AWS controls and processes all IoT data
Long-Term Costs	Predictable and fixed, no reliance on external providers	AWS pricing may increase, leading to unexpected costs

So, by optimizing blockchain transactions with Layer 2 scaling solutions (e.g., rollups, sharding), we achieve lower costs and faster speeds than AWS IoT. Unlike AWS IoT, which incurs hidden costs and depends on a centralized infrastructure, blockchain enables efficient, low-cost, and high-speed transactions with greater security and transparency. Table 2 highlights blockchain's advantages over AWS IoT.

8. PRIVACY-ENHANCING TECHNOLOGIES (PETS) FOR BLOCKCHAIN-BASED IOT SYSTEMS

Privacy-Enhancing Technologies (PETs) play a crucial role in balancing privacy and usability, particularly in blockchain-based IoT ecosystems, where transparency may expose sensitive information. To mitigate these risks, several cryptographic PETs have been introduced, ensuring data confidentiality without compromising decentralization. One of the most powerful PETs is Homomorphic Encryption (HE), which allows computations on encrypted data without decryption, ensuring that sensitive IoT data remains private, even on public blockchains. First introduced by Rivest, Adleman, and Dertouzos, HE in Eq. (2) ensures that given plaintext space *M*, an encryption scheme HE remains homomorphic over an operation

$$\mathrm{HE}(\mathrm{m1}) * \mathrm{HE}(\mathrm{m2}) = \mathrm{HE}(\mathrm{m1}) + \mathrm{HE}(\mathrm{m2}), \forall \mathrm{m1}, \mathrm{m2} \in \mathrm{M} \qquad (2)$$

HE is classified into:

• Partially Homomorphic Encryption (PHE) – Supports either addition or multiplication, but not both.

• Fully Homomorphic Encryption (FHE) – Supports both addition and multiplication, enabling complex computations on encrypted data.

Other key PETs for blockchain-based IoT include:

• Zero-Knowledge Proofs (ZKPs) – Allow verification of transactions without revealing underlying data, ensuring privacy in IoT data monetization.

• Secure Multi-Party Computation (SMPC) – Enables collaborative data processing across multiple IoT nodes without exposing private inputs.

• Pseudonymization & Anonymization – Methods that decrease the danger of individuality revelation in decentralized IoT networks.

These PETs communally improve confidentiality and safety in BLCH based IoT applications, safeguarding that sensor data transactions keep on trustless, confidential, and confirmable.

9. CHALLENGES

The combination of IoT with BLCH technology offerings numerous challenges that necessity to be talked for effective employment. One of the main challenges is scalability, as the BLCH can develop loaded due to high transaction sizes. For instance, Bitcoin's storing had exceeded 197 GB in 2019 [30], and participating IoT with BLCH would individually enhance extra straining, possibly impairing this issue. One more important challenge is storing. The BLCH record is kept on every IoT node, and as the system balances, the scope of the record rises, making storing loads on each linked node. Handling this development in information is a compound commission and can chief to performance issues. The absence of extensive services is too a main barrier, as BLCH is still a comparatively new technology, and only a minor collection of persons has knowledge in it. This brands exercise and upskilling persons to work with BLCH in IoT applications a vital yet challenging task. In adding, detection and combination attitude problems. BLCH was not originally considered for IoT, and it develops interesting for associated nodes to determine and take part with one another inside the BLCH ecosystem. While IoT nodes can determine each other, launching continuous associates with BLCH based devices needs disabling technical hurdles. Confidentiality remains alternative important concern. Since BLCH record is publicly available to all associated nodes, complex data power be visible, making confidentiality dangers in the combined method. Safeguarding information safety and confidentiality while continuing BLCH transparency is a challenge that needs to be tackled wisely. Interoperability is also a serious issue. With the attendance of both public and private BLCH, safeguarding continuous statement among diverse kinds of BLCH networks inside the IoT setting is essential but hard to accomplish. Finally, as the IoT-BLCH combination may work globally, directing the varied instructions and guidelines leading this method is extra difficulty. Submission with variable allowed frameworks across areas is vital to safeguard the global scalability of the explanation.

10. CONCLUSIONS

This paper discovers the combination of BLCH and IoT, importance individually the prospects and challenges related with this method. We go over many stands supportive this combination and verified how BLCH develops safety, effectiveness, and monetization in IoT networks. By permitting P2P data communications, BLCH decreases costs, removes mediators, and expands actual data entree. As IoT networks remain to raise, the SaaS model suggestions a capable method to data monetization, but its accomplishment be subject to on a safe and well-organized payment structure. Our paper approves that BLCH expertise is a perfect key for this requirement. To confirm this, we proposed a decentralized IoT data market DCAPP using Ethereum BLCOs, where device workers record their devices on the BLCH and operators purchase actual sensor data. Our performance evaluation demonstrated at least 30% faster transactions than centralized IoT cloud systems, processing in 0.3 – 1 second, compared to 0.7 – 1.3 seconds in AWS IoT. Additionally, BLCH based transactions reduced costs significantly, reaching as low as $0.0001 per transaction, making it a cost-effective alternative. Security evaluations showed that BLCO-based transactions prevented unauthorized data modifications, while 85% of users reported greater trust in data security due to BLCH transparency and immutability. Despite these advantages, some challenges remain. Occasional transaction confirmation delays persist, though BLCH scalability solutions (e.g., rollups, sharding) are expected to improve this. Another challenge is preventing fraudulent sensor registrations, which requires additional security measures beyond BLCOs. Future work will focus on integrating privacy enhancing techniques such as homomorphic encryption and zero-knowledge proofs to protect sensitive IoT data while maintaining decentralization and security. Additionally, we aim to expand the application of our BLCH based system to industrial and medical IoT devices, beyond the current focus on weather sensors. In conclusion, our study provides strong

empirical support for the claim that BLCH revolutionizes IoT ecosystems by improving security, decentralization, and monetization. As BLCH scalability and privacy solutions continue to evolve, it is well positioned to become a foundational technology for secure, real-time IoT applications.

REFERENCES

[1] Melesse, T.Y., Orrù, P.F. (2025). The digital revolution in the bakery sector: Innovations, challenges, and opportunities from Industry 4.0. Foods, 14(3): 526. https://doi.org/10.3390/foods14030526

[2] Ali, F.I., Ali, T.E., Al-Dahan, Z.T. (2023). Private backend server software-based telehealthcare tracking and monitoring system. International Journal of Online Biomedical Engineering, 19(1): 119-134. https://doi.org/10.3991/ijoe.v19i01.32433

[3] Eyvazov, F., Ali, T.E., Ali, F.I., Zoltan, A.D. (2024). Beyond containers: Orchestrating microservices with minikube, kubernetes, docker, and compose for seamless deployment and scalability. In 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 1-6. https://doi.org/10.1109/ICRITO61523.2024.10522382

[4] Echefu, G., Batalik, L., Lukan, A., Shah, R., Nain, P., Guha, A., Brown, S.A. (2025). The digital revolution in medicine: Applications in cardio-oncology. Current Treatment Options in Cardiovascular Medicine, 27(1): 2. https://doi.org/10.1007/s11936-024-01059-x

[5] Ragavi, B., Sharmila, S., Kumar, A.M., Kadry, S. (2025). Research challenges and opportunities in blockchain technology. In Blockchain-Based Digital Twins. Apple Academic Press, pp. 37-59.

[6] Wang, X. (2023). Ageing with Smartphones in Urban China: From the Cultural to the Digital Revolution in Shanghai. UCL Press.

[7] Aounzou, Y., Boulaalam, A., Kalloubi, F. (2025). Convergence of blockchain, IoT, and machine learning: Exploring opportunities and challenges–A systematic review. International Journal on Smart Sensing and Intelligent Systems, 18(1): 1-32. https://doi.org/10.2478/ijssis-2025-0002

[8] Rathore, N., Kumari, A., Patel, M., Chudasama, A., Bhalani, D., Tanwar, S., Alabdulatif, A. (2025). Synergy of AI and blockchain to secure electronic healthcare records. Security and Privacy, 8(1): e463. https://doi.org/10.1002/spy2.463

[9] Khan, B.U.I., Goh, K.W., Khan, A.R., Zuhairi, M.F., Chaimanee, M. (2025). Resource management and secure data exchange for mobile sensors using Ethereum blockchain. Symmetry, 17(1): 61. https://doi.org/10.3390/sym17010061

[10] Priya, S.S., Vijayabhasker, R., Rajaram, A. (2025). Advanced security and efficiency framework for mobile AD-HOC networks using adaptive clustering and optimization techniques. Journal of Electrical Engineering & Technology, 20: 1815-1826. https://doi.org/10.1007/s42835-024-02119-9

[11] Kumar, H., Taluja, A., Prasad, R.G., Muniyandy, E. (2025). IoT-cloud-centric smart healthcare monitoring system for heart disease prediction using a gated-controlled deep unfolding network with crayfish optimization. International Journal of Computational Intelligence and Applications, 2450035. https://doi.org/10.1142/S1469026824500354

[12] Kadham, N.R., Krishna, P.G., Ravi, K.S. (2025). IoT-based remote monitoring as a distance (online) laboratory for applied learning. SN Computer Science, 6: 114. https://doi.org/10.1007/s42979-024-03649-9

[13] Ali, T.E., Ali, F.I., Abdala, M.A., Norbert, P., Tejfel, M., Zoltán, A.D. (2023). Exploring application deployment on edge solutions: A focus on mobile edge computing, Akraino Eliot, EdgeX, and OpenVINO for healthcare applications. In Proceedings of International Conference on Recent Innovations in Computing, ICRIC 2023, pp. 851-862. https://doi.org/10.1007/978-981-97-3442-9_60

[14] Suganya, R., Sujithra, L.R., Ayyasamy, R.K., Chinnasamy, P. (2025). Wireless mmWave communication in 5G network slicing with routing model based on IoT and deep learning model. Transactions on Emerging Telecommunications Technologies, 36(2): e70071. https://doi.org/10.1002/ett.70071

[15] Kait, R., Kaur, S., Sharma, P., Ankita, C., Kumar, T., Cheng, X. (2025). Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities. Expert Systems, 42(1): e13561. https://doi.org/10.1111/exsy.13561

[16] Raouf, M.A. (2024). Decentralizing IoT data ownership and control with blockchain technology. In 2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT), Mashhad, Iran, Islamic Republic of, pp. 124-129. https://doi.org/10.1109/SCIoT62588.2024.10570130

[17] Bordel Sánchez, B., Alcarria, R., Ladid, L., Machalek, A. (2024). Using privacy-preserving algorithms and blockchain tokens to monetize industrial data in digital marketplaces. Computers, 13(4): 104. https://doi.org/10.3390/computers13040104

[18] Zhou, L., Diro, A., Saini, A., Kaisar, S., Hiep, P.C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80: 103678. https://doi.org/10.1016/j.jisa.2023.103678

[19] Shafik, W. (2024). Blockchain-based internet of things (B-IoT): Challenges, solutions, opportunities, open research questions, and future trends. In Blockchain-Based Internet of Things. Chapman and Hall/CRC, pp. 35-58.

[20] Trivedi, C., Rao, U.P., Parmar, K., Bhattacharya, P., Tanwar, S., Sharma, R. (2023). A transformative shift toward blockchain-based IoT environments: Consensus, smart contracts, and future directions. Security and Privacy, 6(5): e308. https://doi.org/10.1002/spy2.308

[21] Ali, T.E., Ali, F.I., Abdala, M.A., Morad, A.H., Gódor, G., Zoltán, A.D. (2024). Blockchain-based deep reinforcement learning system for optimizing healthcare. Infocommunications Journal, 16(3): 89-99. https://doi.org/10.36244/ICJ.2024.3.9

[22] Choudhury, B., Singh, P.K., Nath, P., Roy, U., Kalla, A. (2025). Blockchain and smart contract for decentralized and secure spectrum management toward 6G–Beyond hype. Intelligent Spectrum Management: Towards 6G, 211-236. https://doi.org/10.1002/9781394201235.ch9

[23] Ali, T.E., Ali, F.I., Pataki, N., Zoltán, A.D. (2022).

Forecasting cryptocurrency prices using advanced machine learning techniques. In SQAMIA 2024: Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications, Novi Sad, Serbia, pp. 1-11. https://ceur-ws.org/Vol-3845/paper04.pdf.

[24] Ali, T.E., Ali, F.I., Dakić, P., Zoltan, A.D. (2025). Trends, prospects, challenges, and security in the healthcare internet of things. Computing, 107: 28. https://doi.org/10.1007/s00607-024-01352-4

[25] Ali, T.E., Zoltan, A.D. (2025). Hierarchical deep learning for robust cybersecurity in multi-cloud healthcare infrastructures. Engineering, Technology & Applied Science Research, 15(1): 20358-20366. https://doi.org/10.48084/etasr.8918

[26] Pokharel, B.P., Kshetri, N., Sharma, S.R., Paudel, S. (2025). BlockHealthSecure: Integrating blockchain and cybersecurity in post-pandemic healthcare systems. Information, 16(2): 133. https://doi.org/10.3390/info16020133

[27] Ali, T.E., Ali, I.F., Morad, A.H., Abdala, M.A., Zoltan, A.D. (2024). Diabetic patient real-time monitoring system using machine learning. International Journal of Computing and Digital Systems, 16(1): 1123-1134. http://doi.org/10.12785/ijcds/160182

[28] Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Muthukkumarasamy, V. (2020). A survey on blockchain-based platforms for IoT use-cases. The Knowledge Engineering Review, 35: e19. https://doi.org/10.1017/S0269888920000284

[29] Al Sadawi, A., Hassan, M.S., Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access, 9: 54478-54497. https://doi.org/10.1109/ACCESS.2021.3070555

[30] Ashfaq, M.T., Javaid, N., Alrajeh, N., Asim, Y., Akber, S.M.A. (2025). Scalable hybrid deep models for individual pharmacy cost prediction. IEEE Access, 13: 31912-31935. https://doi.org/10.1109/ACCESS.2025.3541750

NOMENCLATURE

B	dimensionless heat source length
CP	specific heat, J. kg^{-1}. K^{-1}
g	gravitational acceleration, $m.s^{-2}$
k	thermal conductivity, $W.m^{-1}$. K^{-1}
Nu	local Nusselt number along the heat source

Greek symbols

α	thermal diffusivity, m^2. s^{-1}
β	thermal expansion coefficient, K^{-1}
ϕ	solid volume fraction
Θ	dimensionless temperature
μ	dynamic viscosity, kg. m^{-1}. s^{-1}

Subscripts

p	nanoparticle
f	fluid (pure water)
nf	nanofluid