International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6316
***Article Received**: 24 December 2022 **Revised**: 31 January 2023 **Accepted**: 08 February 2023*

Digital Hash Data Encryption for IoT Financial Transactions using Blockchain Security in the Cloud

T. Blesslin Sheeba[1], S.V. Hemanth[2], V. Devaraj[3], A. N. Arularasan[4], M. Gopianand[5]

[1]Department of ECE, R.M.K. Engineering College,Kavaraipettai, Thiruvallur District- 601206, Email: tbs.ece@rmkec.ac.in

[2]Associate Professor, Department of Computer Science and Engineering,Hyderabad Institute of Technology and Management,Medchal-Malkajgiri, Telangana 501401,India. Email: hemanth.sandapaga@gmail.com

[3]Associat Professor, Department of Electrical and Electronics Engineering, Panimalar Engineering college,Poonamallee, Chennai, Tamil Nadu 600123, India, Email: djran14@gmail.com

[4]Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai - 600 123, India, Email:arularasan@live.co
(Corresponding Author)

[5]Department of Computer Applications, PSNA College of Engineering and Technology,Dindigul.Tamilnadu-624622, India.Email: mgopianand@psnacet.edu.in

Abstract— Blockchain security via the Internet of Things (IoT) will reshape the decision-making function of the data-driven incumbent smart enterprise, providing the vision of the connected world of things. Enterprise IoT development of devices, personnel, and systems in such a way that they may connect and communicate with each other through the Internet. Blockchain is an enterprise financial transaction, and its digital network is distributed transaction ledger. Today, enterprises need the massive global data management and rapid trading volume to keep things going and growing. It creates enterprise business challenges of different types of security, transparency, and complexity of the problem. Enterprise architecture offers several advantages for the thief to obtain a specific user account, application, and access to the device. This is, will doesn't be to provide the necessities of security. The proposed Digital Hash Data Encryption (DHDE) is used to secure the transaction data-based embedded system people and blockchain. Blockchain and IoT technology integration may bring numerous benefits to mention. Therefore, the proposed DHDE algorithm comprehensively discusses the blockchain technology integration system. The proposed DHDE algorithm encrypts the transaction data for an unauthorized person who cannot access the enterprise transaction data based on embedded system people and blockchain.

Keywords- Internet of Things (IoT), Blockchain, transaction ledger, Digital Hash Data Encryption (DHDE), enterprise, security**.**

I. INTRODUCTION

With the advancement of science and innovation and the adjustment of individuals' insight, the capacity and handling of information are continuously moving to online activity. Even though the presentation is improved, it can make hopeless misfortunes due to noxious assaults by aggressors. Financial, clinical and managerial positions would only exist with its help. Information breaks happen once in a while. Gadgets associated with the Web store a lot of individual information. Blockchain is one of the problem areas as many organizations begin to track down better approaches to store and fabricate confided in web-based biological systems to protect this information. Bitcoin's appearance denotes a tipping point in a prickly social peculiarity, with the progressive change in the centre from conventional data sets to get capacity inside blockchains. Various applications because of blockchain innovation have arisen. Executing blockchain from a security perspective no longer addresses the issues of everyday tasks. Subsequently, it merits thinking about creating blockchain applications with low utilization, high comfort and adaptability while guaranteeing blockchain security.

Development is predominantly reflected in two viewpoints: first, the topic is somewhat new, and specialized examination is more definite. The analysis of blockchain and its applications is still at its outset. It investigate and present the blockchain innovation's specialized engineering, lopsided cryptography and blockchain security reaction component in as much detail as possible, which has yet to be found in current scholarly papers. Second, the test examination tells the truth. As the exploration of blockchain innovation keeps on extending, tests in many fields have slowly begun, and there is something else and more cases for examination and examination. Because of crucial security trade testing and analysis, blockchain innovation has a high reasonable significance to work on conventional models.

The proposed DHDE algorithm is based on embedded systems and blockchain to encrypt the transaction data to unauthorized persons who cannot access the enterprise transaction data.

The proposed way to deal with getting outsider financial exchanges using distributed computing includes a primary cycle and requires multifaceted confirmation of errors in exchange records put away on a blockchain. The proposed engineering lessens the encryption and unscrambling costs and gives high security to outsider exchanges. This segment characterizes the means engaged with the proposed strategy for secure blockchain-based outsider exchanges through distributed computing.

To meet the developing necessities of blockchain clients in finance, blockchain utilizes decentralized data sets, while customary financial frameworks use.

Concentrated data sets with a solitary mark of affirmation. Rather than depending on a solitary assent framework, clients with suitable assents can get records from numerous frameworks. Smart contracts, self-executing arrangements that uphold recently arranged structures, are a vital element of blockchains.

A. Contribution of this work

- Design a framework to implement multi-factor authentication processes to detect inconsistencies in user service request patterns.
- The proposed work involves a blockchain that combines previous third-party transaction histories to detect user service request pattern discrepancies.
- Reduce the computational time and cost of encryption and decryption during third-party transactions.

II. Related Work

Blockchain has drawn a lot of consideration from the scholarly community because of its decentralization, dependability, namelessness, and audibility. Over the past ten years, blockchain innovation has kept advancing, making it suitable for non-monetary applications [1]. Notwithstanding, most blockchain-appropriated research has zeroed in on open chains and, in this way, can't uphold contract calls, severe exchange atomicity and short accessibility [2].

Block connected Blockchains (BLB) are proposed to utilize the Chameleon hash capability to lay out bidirectional pointers between blocks. Furthermore, another Collecting Membership Transaction (CMT) agreement calculation intends to work on the security and assault opposition of BLB while guaranteeing high adaptability [3]. Blockchain has acquired a lot of consideration lately. In any case, blockchain execution can't fulfil the needs of the enormous number of Internet of Things (IoT) gadgets. One of the significant bottlenecks of blockchain is the restricted processing assets on a server while completing exchanges utilizing Aeolus blockchain [4]. Even so, more is needed about the exchange cost and time-to-activity expectation for blockchain-based frameworks [5].

BlockChain-empowered CED (BC-CED), a blockchain-empowered cooperative offload for CED estimations. In BC-CED, blockchain assumes a significant part in the critical elements of CED, for example, task offloading, intervention, and impetuses for asset usage [6]. Its fruitful use in digital forms of money, empowering activities in business, modern and administration frameworks, upheld by functional choices given by Ethereum shrewd agreements and public-private key cryptographic security, I had the option to investigate [7]. Be that as it may, customary block-based blockchain innovations, for example, Bitcoin and Ethereum, are inadmissible for IoT conditions because of their low presentation, high computational above, and high exchange expenses [8].

Blockchain has been acquiring consideration for its potential applications in the Web of Things (IoT) space. Information is put away in permanent blocks related to secure shared, especially in the developing exchange check issue in modern and administration conveyance applications [9]. The IoT environment incorporates information suppliers, for example, sensors and applications that require monetary exchanges to remunerate information makers. This shows the significance of IoT instalments and commercial centres to work with miniature exchanges across billions of associated gadgets in a different, decentralized, and complex IoT biological system [10].

A blockchain-based internet business exchange legal sciences stage, this standard portrays specialized reference structure, essential functional prerequisites and specialized markers [11]. Dispersed energy is a significant innovation that helps the improvement of clean energy. Be that as it may, the current conveyed energy networks have issues, for example, restricted relevance, slow improvement speed, and low unwavering quality [12]. An insightful model assessed the handling execution given the lining hypothesis to appraise the typical exchange affirmation time. It measures information respectability through reenactments and evaluates the chance of harming put-away information currently [13]. A decentralized energy proprietor fit for energy creation, and utilization is characterized as able [14]. Most existing BaaS frameworks are facilitated in cloud supplier conditions, which likewise represent the gamble of seller security, subverting the innate unwavering quality of blockchain. Facilitate Peer-To-Peer (P2P) energy trading between presumes, blockchain is flourishing as a technology used in P2P networks due to its transparency, security and speed of transaction processing [15].

III. Proposed Method

The use of blockchain tools involves designated persons to ensure customer privacy. Blockchain use various security schemes to lock down the information contained in the blocks. Secure the cloud using Digital Hash Data Encryption (DHDE) algorithm-based banking algorithms. It describes the characteristics of the cloud and its security challenges in the

***Article Received**: 24 December 2022 **Revised**: 31 January 2023 **Accepted**: 08 February 2023*

banking sector. The integration of Blockchain and IoT technologies offers many benefits. Therefore, the proposed DHDE algorithm provides a detailed discussion of the integrated structure of blockchain technology.

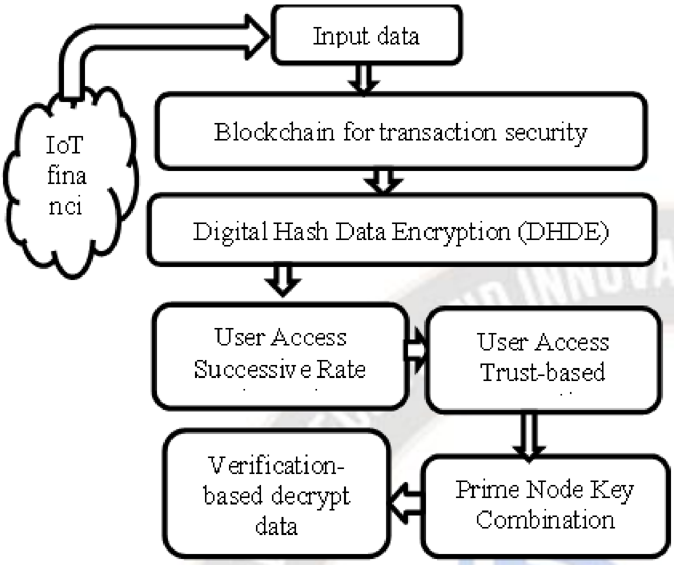
Input data
IoT fina nci
Blockchain for transaction security
Digital Hash Data Encryption (DHDE)
User Access Successiv e Rate
User Access Trust-based
Verification-based decrypt data
Prime Node Key Combination

Fig.1 Proposed Architecture for Blockchain _IoT Security

Fig.1 describes, proposed block diagram for Blockchain Security in Cloud Computing Based on Key Additions, Early Node Integration for Encryption for Secure Access, and Proposals for Transactions and Authentication in IoT Cloud Computing encrypted using Digital Hash Data Encryption.

A. *Blockchain security for the financial industry*

Blockchain facilitates the safe and efficient sharing and management of financial transaction records using smart contracts. Smart contracts rely on financial records management and are the subject of a particular application of blockchain in smart finance transactions. It implements a structure using the DHDE algorithm. Blockchain is chosen for the seamless sharing and storage of financial data. Banking systems are prone to problems leading to increased costs and poor business results. The solution is protection. Blockchain technology is being touted as a convenient tool for managing data confidentiality, privacy and security, especially in the banking industry. Blockchain uses cryptographic hashing technology to protect the financial record and prevent data leakage.

- A blockchain-based framework that secures and verifies the healthcare sector's record-sharing system.
- The primary purpose of our work is to secure Financial Transaction Records (FTRs) and use the blockchain to ensure that FTRs are shared and stored in the cloud.
- Use hashing techniques with the DHDE algorithm to generate hash values, verify data integrity, and use hashing techniques to verify records.
- Use sensors to collect and store sensor data in cloud-based storage, making the data irreversible.

B. *User Access Successive Rate (UASR)*

User Access Successive Rate (UASR) is based on digital identity verification, record authentication and blockchain. It enables more efficient and secure authentication and UASR while respecting the identity holder's identity than traditional identity systems. Using a blockchain trust framework, a blockchain-based identity system eliminates intermediaries, waiting for authentication and authorization queues. The source of the stack source enables the user-proof link. It is optional to calculate a large number of hashes to create a chain with a high block rate to find the correct hash.

```
Algorithm steps: User Access Success rate
User Hash Insert (R, S, M)
    H🡨Hash (R.Get user Name ())
If H. Contains Key (H), then
    J🡨 H.Get (H)
If is Pair (R, S), then
            S. Insert ((R, S))
Else List Insert (R, S, M)
            H.insert (H, R)
Else
    H. Insert (H, R)
            Add R to H
Schedule a file size < Point of some file
Access Max. Original file (H)
End if
End if
End
```

Where the H-Hash key, J- variable, R, S, and M-User Successive Rate use responses from the source, the long key principle, and peer validation to ensure that user roles within a block consent to each size elevation.

C. *User Access Trust-based encryption (UATBE)*

In a cloud environment, many users access services and data that reside in the cloud. The cloud contains different data belonging to different users and clients. Users should be restricted from accessing other data they do not have access to. It can be implemented through UATBE-based access controls. Every time a user requests access to specific data, it allows the use of profile classification to check the user's access against all required attributes. Similarly, user behaviour while accessing the data is used to measure UATBE metrics. The value of UATBE limits the key.

Input: trace (T), request (r), and profile classification P.C.
Output: Boolean Trust Values

```
    The starting point
    D, R, B.D. Read. // Place to keep track of (T), request (r), profile classification Pc
    Data Identifying Demand (DI) = (D.i.)
    Give the data
    Classify the desired features in Fl using the following expression: feature list Fl = Pro. Features
    Use expressions to identify accessible features
    : Access Feature List (AFL) =
        $\int_{x=1}^{siz\ (PC)} \int_{x=1}^{size(Fl\ )} \mathrm{Fl}\ (y) \in \mathrm{PC}(x).\mathrm{Usr} == \mathrm{U}$
    Compute Earlier Access Trust (EAT) value using the equation: Earlier Access Trust EAT
    $\frac{\sum_{x=1}^{size(T)} T(x).Usr==u\ \&\&T(x).Access=complete}{\sum_{x=1}^{size(T)} T(x).Usr==u}$    (1)
    Calculate UATBE Evaluate using Eq.
UATBE=$\frac{Size(AFL)}{Size(FL)}$XEAT    (2)
If UATBE $>$ T, then
Return true.
Else
Return false.
End
```

Restricting access using the UATBE algorithm is based on the UATBE metric computed for a particular user request. This method restricts access to users depending on the UATBE value.

```
    Encryption
    Features= Encrypt (Fe, E.Fe. E.Key.)
        End for
    Encrypted data (Ed) = combine (F)
    Random(R) =$\int$ random(4,10)
    Data count (Dc) =$\int$ Sep(Ed, R)
        Initiate Blockchain (B.C.)
    Generate Dc (No.blocks (Nb))
        $\mathrm{Bc} = \int_{x-0}^{size(DI)} \sum(\mathrm{blocks} \in \mathrm{Bc}) \cup \text{generate blocks}$
            (3)
    End
```

This method uses a different encryption method and key to encrypt each property. Furthermore, data is divided into several blocks. Blockchain is generated based on the number of blocks.

D. BlockChain Generation

Once the cloud is accessed, and the required data is extracted, the blockchain generation scheme is executed. Once the user has been granted access, the method accesses the data and retrieves the needed data. This method extracts user-accessible properties from data.

```
    Input: Data (D), Access Feature Count (AFC), Attribute Classification (A.C.)
    Output: Block Chain (BC), Data blocks (DB)
    Begin
    Read D, AFL, AT. // Data D, Access Feature Count (AFC), Attribute Classification AC

    Extracting Features (F) = $\int_{x=1}^{size(D)} \sum \mathrm{D}(x) \in \mathrm{AfL}$
                                                        (4)
        For All feature (F) of fes
        D.O.
    Select Encryption (Es) = $\int_{x=1}^{size(at)} \mathrm{Random}(at(x).f) == F, at(x).\text{Selected values})$    (5)
    Select Encryption keys (Eks) = $\int_{x=1}^{size(at)} \mathrm{Random}(at(x).f) == F, at(x).\text{Selected keys})$
                                            (6)
```

Presently select a remarkable encryption strategy and key from the arrangement of techniques and keys utilizing the property class AT. The encryption plot and the created key scramble information properties. Likewise, this strategy makes an irregular number R from the set Z*P. This addresses the quantity of blocks produced in the chain. In view of the worth of R, the technique will produce the blockchain and partition the information into R blocks. Dynamic block-level encryption and unscrambling utilizing the created blockchain and information blocks.

E. *Digital Hash Data Encryption*

The blockchain hash every one of the trades prior to pressing them into blocks. Hash Pointers associate each block with its past block by holding a hash of the data in the past block. Each block is connected to the past block, so the data in the blockchain stays unaltered. A hash capability implies organizing any trade will give a one-of-a-kind hash and modification of the hash of every ensuing block, and it contains hash code.

$$\text{Hashing f uction (Index } + \text{ Previous Hash value } + \text{ Timestamp } + \text{ Data } + \text{not once value) } = \text{ Current Hash value} \qquad (7)$$

The not-once value is used to find valid hashes. Therefore, need to find a nonce value that produces a valid hash when used with the rest of the information in that block.

The recipient can get a code that recognizes the encryption key utilized from the hash code. By distinguishing the key, the recipient can decode the cipher text and recover the first information. The proposed framework uses a key set containing the number of keys for information encryption. A plan of primes and polynomials performs the key determination. This technique utilizes a person set that includes different endless letters. Keysets and charsets are dispersed to clients at the underlying stage. To begin with, the method creates an irregular number in view of the size of the charset utilized.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6316
***Article Received**: 24 December 2022 **Revised**: 31 January 2023 **Accepted**: 08 February 2023*

```
    Input: Singe set (cs), Key set (ks), Information (d)
    Output: Hashing code (Hc), Encode txt (E.T.)
    Start
        Recognize cs, ks, d
$R1 = \int random\ (1, size(cs))\ //add\ limit$
$Char\ (y) = Cs\ (R1)$
    If y (prime)
    Then
        $Generate\ Hash\ cipher\ = y +$
 $Random\ (size\ (keyset)))$
    $Encrypt\ data\ (Ed)\ =\ Encode\ (keyset\ (ASCII(y) -$
$Random\ size\ (keyset))$                    (8)
    End if
    End
```

The resulting hash code is then added to the considered block, and the encrypted data is added to the block. Based on the hash code, users can identify the key that is used to decrypt the text and recover the original data.

4. Result and Discussion

This section presents the proposed experimental results run in C#.net language and visual studio tool. The proposed algorithm Digital Hash Data Encryption (DHDE) compared with the existing approach.

Table 1 Simulation Parameters

Proposed Parameters	Simulation Values
Tool	Visual Studio 2017
Language used	C#
Number of users	750
File Size	500MB

Table 1 presents Simulation parametric metrics for evaluating proposed algorithms. The comparative parameter metrics for the proposed algorithms are transactional security accuracy performance, file encryption/decryption performance, transactional access control analysis and latency.

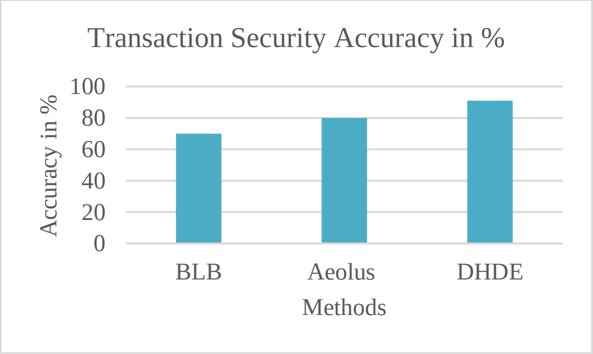

Fig. 2. Analysis of Transaction Security Accuracy

Fig.2. defines the analysis of Transaction Accuracy performance based on proposed and existing results. The proposed Digital Hash Data Encryption (DHDE) algorithm security performance is 91%. The proposed algorithm enhances the security performance compared with the existing algorithm.

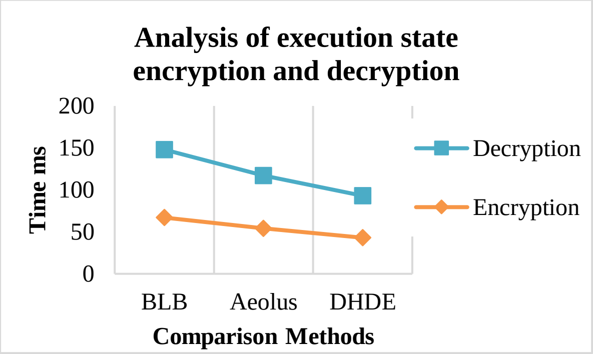

Fig.3. Analysis of execution state encryption and decryption

Fig.3. defines the analysis of execution state encryption and decryption performance comparison results. The proposed DHDE algorithm produces a low time performance than existing algorithms. The proposed DHDE algorithm encryption and decryption is low time.

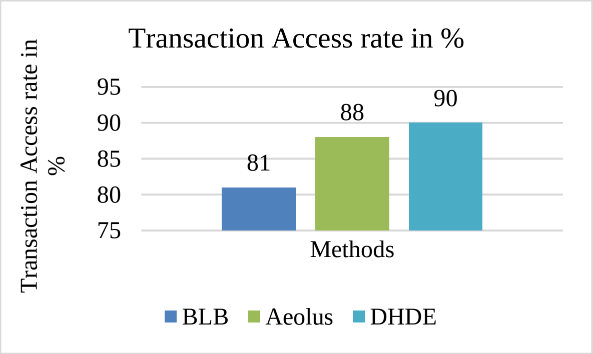

Fig.4. Transaction Access Rate Analysis

Transaction Access Rate Analysis comparison results are shown in fig.4. The proposed DHDE algorithm performance is 90%. Likewise, the existing algorithm is better than the previous methods.

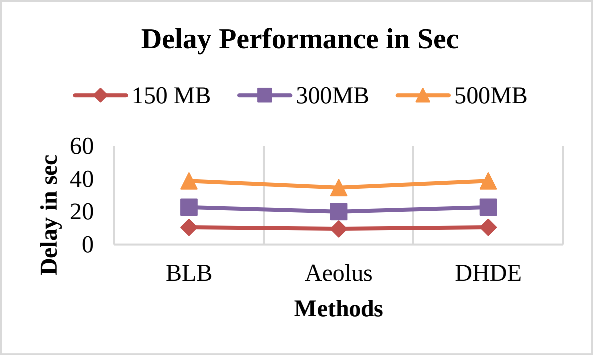

Fig.5 Latency performance

Fig.5. defines the analysis of delay performance comparison results. The proposed DHDE algorithm has 16 sec for a 500MB file size. Similarly, the proposed algorithm is better than the previous 500MB file size algorithm.

IV. CONCLUSION

To address the issue of security and fairness in data transactions, measures have been proposed to ensure the fairness and security of data transactions through a trusted third party or arbitrator. However, these propositions are vulnerable to single points of failure and can leak useful data information. Design a fair and verifiable data exchange program that does not require third-party participation. The entire process of data transactions happens between data owners and data consumers only. Intelligent contracts take full advantage of blockchain technology's decentralized and immutable capabilities, where all transaction data is uploaded to the chain and personal data business operations, and sharing is complete. After the data owner receives the coin, the data consumer immediately gets the encryption key, and the intelligent contract writes the transaction record to the blockchain for easy tracking. The proposed solution uses blockchain, which has excellent properties such as tamper resistance but inadequate data processing efficiency. Future research will improve the theory and methods of blockchain operational efficiency, i.e. use more efficient methods and explore the possibility of trading off security and efficiency in blockchain to improve project efficiency further. Also, in fair and verifiable data trading schemes, data verification schemes can guarantee data reliability but cannot fully ensure that false data will not damage data.

REFERENCE

[1]. W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in IEEE Access, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.

[2]. P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Multiple Execution Environments Per Organization in Sharded Consortium Blockchain," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3562-3574, Dec. 2022, doi: 10.1109/JSAC.2022.3213326.

[3]. C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm For Internet Of Things," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4371-4384, 15 March15, 2022, doi: 10.1109/JIOT.2021.3103275.

[4]. P. Zheng et al., "Aeolus: Distributed Execution Of Permissioned Blockchain Transactions Via State Sharding," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.

[5]. Welligton dos Santos Abreu, E. F. Coutinho and C. Ilane Moreira Bezerra, "Performance Evaluation Of Data Transactions In Blockchain," in IEEE Latin America Transactions, vol. 20, no. 3, pp. 409-416, March 2022, doi: 10.1109/TLA.2022.9667139.

[6]. S. Yao et al., "Blockchain-Empowered Collaborative Task Offloading For Cloud-Edge-Device Computing," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3485-3500, Dec. 2022, doi: 10.1109/JSAC.2022.3213358.

[7]. F. D. Giraldo, B. Milton C. and C. E. Gamboa, "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept," in IEEE Latin America Transactions, vol. 18, no. 10, pp. 1743-1751, October 2020, doi: 10.1109/TLA.2020.9387645.

[8]. T. Wang, Q. Wang, Z. Shen, Z. Jia and Z. Shao, "Understanding Characteristics And System Implications Of DAG-Based Blockchain In IoT Environments," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14478-14489, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3108527.

[9]. A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol For A Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.

[10]. A. Saputhanthri, C. De Alwis and M. Liyanage, "Survey On Blockchain-Based Iot Payment And Marketplaces," in IEEE Access, vol. 10, pp. 103411-103437, 2022, doi: 10.1109/ACCESS.2022.3208688.

[11]. Treiblmaier and Sillaber. “The Impact Of Blockchain On E-Commerce: A Framework For Salient Research Topics,” in Electronic Commerce Research and Applications, pp.1-12,Aug.2021, doi:10.1016/j.elerap.2021.10105

[12]. Z. Liu, H. Pang, Y. Li and S. Li, "Research On Distributed Energy Network Transaction Model Based On Blockchain," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), 2021, pp. 311-314, doi: 10.1109/CBFD52659.2021.00069.

[13]. C. K. Da Silva Rodrigues and V. Rocha, "Towards Blockchain For Suitable Efficiency And Data Integrity Of Iot Ecosystem Transactions," in IEEE Latin America Transactions, vol. 19, no. 7, pp. 1199-1206, July 2021, doi: 10.1109/TLA.2021.9461849.

[14]. Z. Cai et al., "RBaaS: A Robust Blockchain As A Service Paradigm In Cloud-Edge Collaborative Environment," in IEEE Access, vol. 10, pp. 35437-35444, 2022, doi: 10.1109/ACCESS.2022.3161744.

[15]. J. Yang, A. Paudel and H. B. Gooi, "Compensation For Power Loss By A Proof-Of-Stake Consortium Blockchain Microgrid," in IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3253-3262, May 2021, doi: 10.1109/TII.2020.3007657.