Synthesis: A Multidisciplinary Research Journal
Volume 3, Issue 4, October – December 2025, Pp: 54-65

Research Paper

Secure Blockchain-Based Consumer Electronics Platform for Smart Homes with Efficient Access Control and Performance Evaluation

[1*]Srinivasarao Goda, [2]Pratap Pachipulusu, [3]Sakhamuru Amulya,Pathan Hussian Basha

*[*1]Associate Professor, Department of CSE, RVR&JC College of engineering Guntur, Andhra Pradesh, India. Email ID: gsraob4u@gmail.com*
[2]Data engineering and AI ,Walmart Inc, Bentonville, AR, USA, e-mail: pratap.pachipulusu3@gmail.com.
[3]Engineer IV, Collegeboard, 11955 Democracy Dr, Reston, VA 20190, USA Email ID: asakhamuru@collegeboard.org
[4]Department of Computer Science and Engineering, PACE Institute of Technology and Science, Valluru, Ongole, Andhra Pradesh, India. Email ID: phussain786@gmail.com

**Corresponding Author(s): gsraob4u@gmail.com*

Article Info

Received: 19/09/2025
Revised: 26/11/2025
Accepted:15/12/2025
Published:31/12/2025

Abstract

Blockchain technology has emerged as a pivotal solution in contemporary digital ecosystems, addressing challenges ranging from supply chain management to the preservation of data integrity. One prominent application domain is consumer electronics, where smart homeowners increasingly rely on interconnected devices to access services in a seamless and efficient manner. While these technologies significantly enhance convenience and quality of life, they also introduce critical security and privacy concerns due to data sharing, unauthorized access, and potential cyberattacks. Addressing these challenges requires robust and reliable security mechanisms that ensure trust and transparency. This study proposes a smart and secure blockchain-based framework tailored for consumer electronics platforms, with a primary focus on identifying potential security threats and mitigating them through appropriate blockchain solutions. A set of practical case studies is presented to demonstrate how blockchain can enhance secure service access while maintaining data authenticity and resistance to tampering. The proposed framework is implemented and evaluated using a private Geth network, enabling controlled experimentation and performance analysis. Performance evaluation primarily focuses on the time required for data loading, retrieval, and block access operations. Experimental results indicate that the proposed Blockchain-Based Consumer Electronics Store (B2CES) exhibits a steady and linear increase in processing time as the number of items scales from 1 to 500, ranging from 0.10 seconds to 8.60 seconds. This performance demonstrates improved efficiency when compared to existing approaches, which exhibit a sharper increase from 0.38 seconds to 9.29 seconds for similar operations. Furthermore, block access time for a set of 500 items is reduced to 7.12 seconds in the proposed framework, compared to 9.29 seconds in conventional implementations. These results confirm the effectiveness of the proposed blockchain solution in achieving enhanced security with reduced computational overhead.

Keywords: Blockchain technology, Consumer electronics, Smart homes, Data security, Access control, Performance evaluation.

1. Introduction

Blockchain technology often comprises of inbuilt security such as hashing the original data and recording inside the blocks to deal with voluminous data sizes. However, the criticality of the data defines the strength of security to be incorporated inside the contracts to eliminate unauthorized access. This also depends on the nature of the blockchain platform under consideration as per the use-case implementation [1]. For example, if a blockchain is to be set up for social networking platforms, then the security aspects need not necessarily be as stringent as needed for the credit transactions made by an individual.

The higher the security, more will be the cost incurred towards maintenance of the environment where the work is being carried out. Hence, it is essential to identify the nature of the data to be analyzed and the relevant attributed to be encryption via the adoption of a suitable security algorithm, before proceeding with the process execution phase. This also involves elimination of the isolated nodes and untrustworthy nodes from the network which are found to malfunction and distract all other participating entities [2]. However, the layer at which security must be imposed is a crucial decision to work on to develop smart contracts accordingly. The inculcation of distributed technologies in providing various services ranging from drug discovery to electricity consumption in a fare-based environment is at a rise. This usage stands better when deployed via blockchain technology to keep away miscalculations and mutable data strategy. Contracts or chain codes are written in a way where timely assessment is made on the data access and retrieval policy by the authorized users connected across the network. This aspect adds great weight to the households to overcome additional cost and unnecessary penalties in terms of service consumption irrespective of the application [3]. However, while the emphasis is on the elimination of mutable aspects, the nature of consensus algorithms to be developed in compatibility with the system is an essential but challenging task.

The existence of a wide number of consensus algorithms to achieve a common agreement across a set of nodes in the block-based network assists individuals to implement secure and flexible user requirements adhering to the applications. However, the identification of a suitable one is a challenging aspect, that needs the internals of an algorithm to be traced out. Also, every consensus algorithm exhibits a unique aspect. Hence, it is difficult to identify one that addresses multiple issues such as scalability, failure-handling capacity, voluminous job execution etc [4].

Towards this end, in this work, the following contributions are made:

1. An analysis is carried out on a series of smart and secure blockchain based case studies for consumer electronics platforms along with an implementation of blockchain in retail industry, Cloud Blockchain Service Access, Blockchain in Smart Home secure service access along with their impact.
2. The significance of Blockchain to prevent online donation frauds, Online Proposal Submission System and Social Networking Blockchain Network is also emphasized on.
3. An implementation of Blockchain Based Consumer Electronics Model is done via blockchain nodes created in Geth and results are obtained to showcase the significance of the proposed B2CES model over the existing non-blockchain based models.

The implementation of the proposed Blockchain Based Consumer Electronics Model incorporates the addition of a set of nodes that accommodate the transactions inside the block. A transaction is triggered in terms of the attributes for consumer electronics. Among all the nodes, 1 is marked to be the admin node and 1 node acts as a malicious one. This strategy helped to achieve the results as demonstrated in the work and make an analysis about the time taken to perform various operations that are found to be improved one over the existing works. Finally, the work is concluded with future insights to address scalability aspects with increasing number of nodes and their capacities to accommodate voluminous transactions respectively.

2. Related Work

In this section, an analysis on a series of smart and secure blockchain based case studies for consumer electronics platforms are presented with prime emphasis on the security attacks that occur on various consumer electronics products respectively. In addition, an implementation of blockchain in retail industry, Cloud Blockchain Service Access, Blockchain in Smart Home secure service access is also presented to identify the significance of proposed B2CES model implementation.

2.1 Secure Blockchain Implementation In Retail Industry

In the retail industry, as the number of users increases, scalability assurance is at stake. The decisions, if dependent on customer feedback, lead to a deterioration of the industry in multiple directions. The decision yielding capacity gets complex if data is arriving across a network of connected devices. Security can be achieved in the retail industry by safeguarding consumer feedback from being manipulated, before being recorded publicly across the media either online or offline, to overcome fake feedback for huge number of products. To strengthen the feedback-based analysis on the past and current user experiences, machine learning integrated with the immutable block network is a suitable platform. The inbuilt consensus has parameters that should be modified to achieve the required performance analysis [5].

In a supply chain firm where the shipping of goods from one end to the other is significant to meet the required estimations, the involvement of fraudulent users at various intermediary phases is another crucial aspect to be focused on. To deal with such aspects, a secure and permitted fabric blockchain is preferable. This enables authorized users to gain access into the private network, with timeframe-based verifications carried out at regular intervals [6]. However, if the nature of data is significantly voluminous, then cloud store can be used to deal with issues emerging out of the defined system.

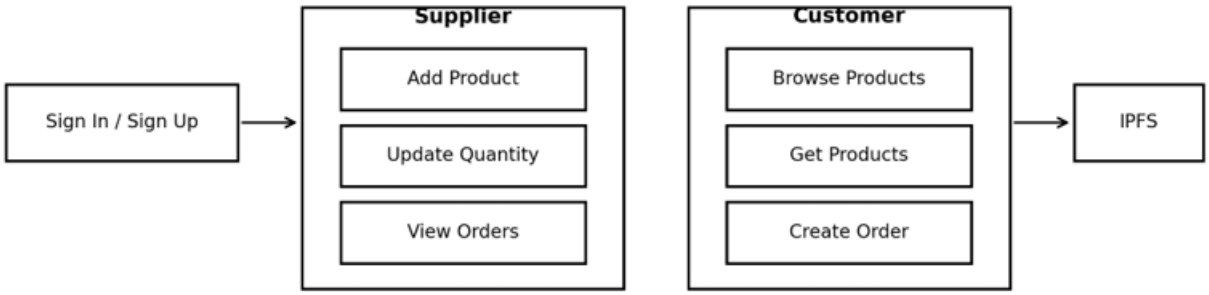

Fig. 1. BC-ecom Architecture

To design a secure consumer access-based system using blockchain, a web or a mobile application with authorized credential-based access provision is a start point. A representation is showcased in Figure 1 which is Blockchain for Ecommerce applications, where, once the user gets through the sign-in procedure, they can add the products to the blocks assigned with the id's, update the accessible quantity, and view a set of orders at their end, when acting as a supplier. At the other end, customers can place orders on the products they are willing to purchase, whose details are recorded inside the blocks. Once the order is confirmed, the transactions are recorded confined to the registered customers [7]. Here, IPFS is a preferable data storage and retrieval repository.

2.2. Cloud Blockchain Service Access

The integration of blockchain with cloud enables scalable service procurement in a cost-effective way. If the data is captured via IoT devices such as sensors across a heterogeneous network, then it is essential to ensure the origin of data from a valid source. Hence, blockchain acts as an efficient means to capture such data via identity verification and validation process. This data is then deployed across the cloud platform to enable multiple users to access within a stipulated time. Though the maintenance of environment can be deployed across the cloud, as the volume of data increases, cost factor is a critical aspect to deal with [8].

An amalgam of clouds with fabric can be carried out in a hierarchical manner where the users are into the front-end interactions at application layer. At the other end, in intermediate layer, a series of executable transactions in a secure way with computing layer-based agreement among the nodes can be established. As there is a limit on the data being accumulated across the nodes, cloud is a preferable environment to address voluminous transactions size, while blocks record only metadata. The data can emerge from across a wide set of heterogeneous sites, that is validated by the authorized entities before getting added to the blocks. If the data to be stored across the blockchain network is non-confidential like the accessible entities of an organizational website, public clouds like amazon web services can be used to deploy the nodes. Else, if confidential data is to be stored, then a private network in azure can be created. However, the maintenance of a private cloud over the public one is a costlier strategy for an individual.

2.3. Blockchain in Smart Home Secure Service Access

When it comes to the smart home environment, security is a prominent aspect to focus on due to the interference of the intruders into the home while using a single key-based access. Immutable block storage of keys is a feasible solution that deals with the problem. This aspect gets more critical if the data to be secured is related to the medical health conditions of the patients residing in a smart home where the enemy tries to gain control over the deployed patient's equipment and harm them. If the healthcare data is collected via sensors, then the adversary may creep into the system and change the data readings. This can be overcome by recording the readings inside the immutable blocks [9].

It is essential to integrate suitable security algorithms into the blockchain environment though it has inbuilt hash-based security. This helps to prevent data from being tampered with. Though an encrypted format is used to store the user credentials, if the hackers who try to gain access into the system are technically sound, they crack the credentials thereby resulting in data stealing and misuse. To deal with such difficulties, if the user credentials are encrypted and recorded inside the blocks at respective hosts as shown in Figure 2, it makes it difficult for the intruders to gain access into the secure and immutable system [10]. However, if the security is incorporated via contracts across the chain network, every modification adds up to the cost factor. Also, the inclusion of IoT devices to collect the data and record it inside the blocks helps to add security as a multi-layer development using key based access. Algorithms such as AES, RSA etc. can be used to ensure confidential access.

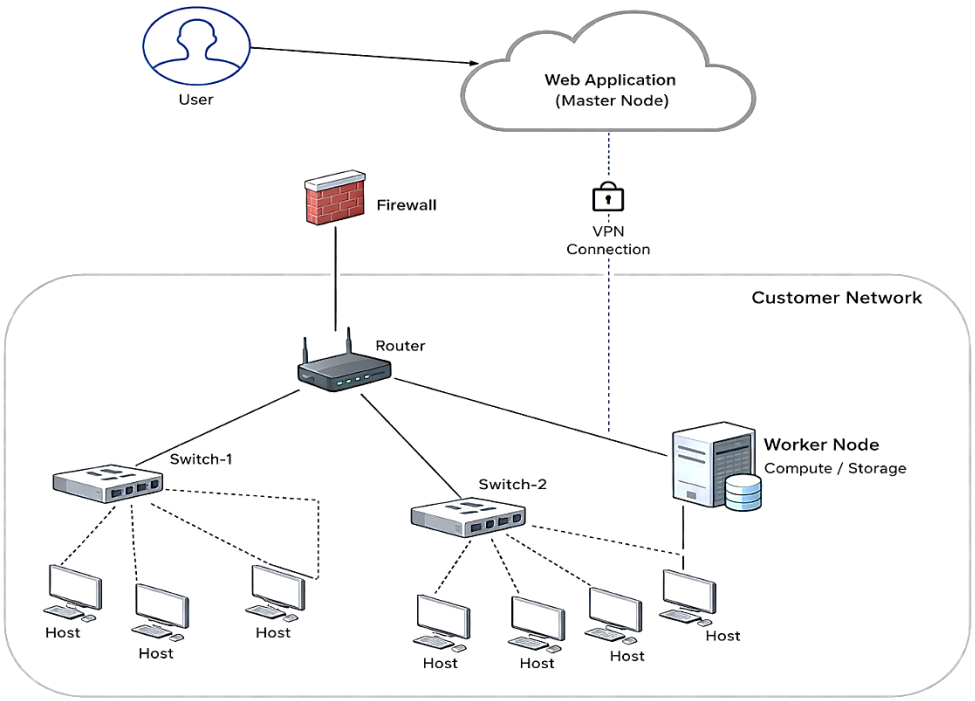

Fig. 2. Blockchain in Smart Home Secure Service

2.4. Blockchain to prevent online donation frauds

Now a days, it is trendy to contribute donations online to help the needy either in the event of natural calamities or to perform rituals or any other necessary contributions. These donations are partially transferred to the authorized person, where the middlemen eat away a significant portion of them. Hence, to overcome the involvement of middlemen during online donations, blockchain technology serves to be a viable platform. Every donation made by an individual is assigned with a unique id as recorded inside the blockchain ledger to promote immutable transaction facility.

Due to lack of knowledge in dealing with the cryptocurrency-based tokens like bitcoins etc., traders hire middlemen to carry out the transactions in a safe manner and at a reduced processing charge. The investors are not worried about losing their earned income towards the charges paid to the intermediaries who safeguard their tokens in the event of messy attacks. This aspect led to the increased demand for middlemen in helping investors. However, if they turn out to be malicious, then the entire hard-earned income is lost. A secure Blockchain platform serves to be crucial to deal with the challenges [11].

The design of a new consensus approach among the participating entities across the blockchain network can be done by writing the Smart Executable Chain Contracts (SECCs). This enables the participating entities to fairly take part in the transaction execution and procure rewards or pay penalties in the event of misfunctioning. This aspect makes it difficult for the intruders to identify the origin of the sender or donor and the receiver of the funds or donations within a stipulated time. This can be set via threshold-based access provision inside the network to identify faulty nodes and immediately block access to them [12]. The authors have created contracts based on the existing FCFS etc algorithms and based on the transaction fee consumed, an efficient one is chosen to make donations.

While there may be a group of youth filled with ideas, either technical or non-technical, to raise profits, they may lag capital to proceed ahead with the implementation aspects. To serve such groups, various crowd funding platforms are moving forward, thereby drawing a considerable portion of the profit earned across the blockchain network connected to entities. Social networking sites are prominent to identify such contributors [13]. However, identification of fake out of genuine contributors is an initial task to be worked on before proceeding further with the contributions.

2.4.1. Social Networking Blockchain Network

There stands a category of users who make donations on a regular basis. The intruders track such people and try to gain unauthorized access to their personal wallets by sharing trojan or viral links. The users may unknowingly click on the link which diverts all their operations to the intruder's accounts. This difficulty can be efficiently addressed using the secure blockchain environment, where every operation is recorded transparently and all log activities remain immutable, leaving no trace for the intruders to erase their virtual footprints.

The relationship between the donators and the amount plays a prominent role in identifying the highly privileged users. This will help the social community to provide suitable offers to the contributors thereby attracting more users to pursue the donations [14]. However, it is essential to maintain an admin-based access provision to such access to keep away intruders.

To overcome a wide set of difficulties related to online donations, many authors developed both web and mobile applications to make it convenient to the technical and non-technical users. Also, a wide number of local languages are added to make it feasible for the users to understand and proceed with the donation process [15]. However, either of

these solutions requires the users to be registered into the system via their unique identification numbers such as Aadhar or pan numbers, to proceed with the donation process. The admin will verify the credentials and assign a unique block id to store the transactions committed by the users.

The involvement of intermediaries is eliminated using blockchain platform that adds up to the productivity to the task initiating entities. It also inculcates the participating entities to keep away malicious behavior due to penalty based smart contracts coded for transaction scenarios across the network [15]. However, the nature of data under consideration is a challenging aspect to be dealt with to address blockchain scalability aspect. It is also essential to assess the backend environment based on the streaming or in-rest data store.

At the other end, not only currency-based donations, but also food donations serve the needy against falling short for food. In the modern days, there are various food donation camps and containers affixed at various locations from where the needy can collect the food items and feed self and family. These camps rely on manual ways of filling in the essential details to proceed with donations, while the nature of donation varies from one event to the other. However, it is difficult to identify the exact locations for the illiterate users to procure the food via maps etc. Hence, to serve the purpose, a blockchain platform with IoT based alert sensors can be developed to send alerts or beeps to the nearby donors and collectors. This system may also prevent animals or other non-humans from destroying the food by recording their features via IoT based deep learning concepts inside the blocks in an unalterable way. There will be a group of people ranging from donors, suppliers to the needy who will all be connected across the blockchain platform for efficient and feasible communication thereby eliminating the paper-based donations [16].

The research in existing domain is widely carried out using the open-source databases to infer productive outcomes. This is associated with data pre-processing approaches to clean the acquired data across a mix of sources and perform analysis. However, to keep away fraudulent access, it is necessary to identify accurate data collection sources across the internet. Otherwise, the obtained analysis will be least significant if data collection sources are non-traceable or identifiable. The nature of donations is also impacted seasonally where in the high percentage of those are from business tycoons [17]. In this direction, the integration of seasonal data analytics on the block data storage yields noteworthy outcomes. Table 1 shows a set of Blockchain based high performance and electronics works existent along with the methodology adopted and lights on the limitations that paved a path to progress with the proposed B2CES model.

Table 1. Existing works on Blockchain based high performance and electronics

Blockchain high performance and electronics based Existing works	Methodology adopted	Limitations identified
An Integrated Blockchain and IoT based tracking system for smart cities [29]	Adopted a distributed file system to store all the e-waste contents in an immutable and transparent manner	Used an insecure Ethereum platform with an emphasis on gas consumption only
Blockchain based enterprise level cost optimization [30]	Uses a scalable BFT for validity verification in a multilevel inventory model	Limited variables from a subset of samples are chosen for correlation analysis and performance estimations
Social perception-based modelling for smart cities growth [31]	Provides an analysis of social intelligence and digital twin mechanism	Theoretical ideas are discussed for intelligent and productive smart city growth, without any emphasis on practical orientation
Ethereum based transaction analysis [32]	Design of an eclipse attack and its probabilistic impact on the data delivery and transfer time	The proposed design is susceptible only towards eclipse attack and does not assure resistance against other types of attacks
A fine-grained blockchain based framework [33]	Hierarchical layer based heterogeneous blockchain systems evaluation based on various performance metrics	The evaluation aspects across cross chain platforms are not considered in the study, that does not ensure scalability aspect
Authentication E-com based blockchain platform [34]	Adoption and implementation of authenticated blockchain platform for varying market requirements	The presented authentication metrics does not span broadly across the supply chain firm and also does not reveal the model behaviour in the event of information asymmetry.

2.4.2. E-Commerce Blockchain

With the selection of blockchain as a suitable environment to keep track of online donations, it is essential that the nodes are deployed against a secure testnet, rather than using a openly accessible platform. The authors in [18] developed a secure system using Ethereum remix testnet where the transaction cost is deducted based on the smart contract execution. However, these contracts are available to all the users without any access restrictions, which may result in insecure code modification and ether tokens theft. Hence, a fabric environment is preferable to develop the online donation system as compared to Ethereum network to ensure secure and authorized entry into the network to make donations or to retrieve the names and address details of the donors to offer privileges and recognitions to them. It is also necessary to identify a suitable data structure to be coded to accommodate all the participating entities and efficient data storage and retrieval aspects.

As crowdfunding is a vast scale environment to gather and update the data across, it is necessary to identify suitable databases that handle such volumes. It is also essential to trace out the nature of donation, whether fixed or random to trace out the regular and irregular donors via machine learning based prediction algorithms [19].

Dependency on social networking sites such as Facebook and Twitter are risk-prone to identify the genuine donors. This system, if built using a secure fabric blockchain platform, enables the users to first verify their

identity and then get connected to the network, thereby building a trustworthy system. This helps eliminate malicious users by recording their identities and matching it with the admin database. If matched, then access is granted, else revoked. Also, the users are assigned with tokens to make donations with the count being incremented for every valid donation. Once the number of donations reaches a certain limit, a reward in the form of a bonus will be credited to the user's account. This facility helps to increase the number of genuine users getting connected into the system [20].

2.5. Blockchain for Online Proposal Submission System

At the other end, in the research proposal submission and call for collaborator's direction, it is a critical task to identify the genuine researchers willing to contribute and get added as a part of the proposal, across socially and publicly viewable platforms. This difficulty can be overcome by assigning a unique identity to every researcher who is going through the advertisement to identify the number of visits made by them to the page, once who read the complete document within a time frame etc. [21]. The data recorded across the blockchain platform will help to identify the malicious and fake users from the log records which are immutable, though the user deletes their entire history of events and pages accessed by them [22].

Based on the nature of data under analysis and criticality, decision about the selection of an accurate platform shall be taken. For example, if the data is gathered manually by conducting reviews, then its size may be small, so any data warehouse or relational database platform may be helpful. At the other end, if the data is gathered across the internet, then it is essential to prefer any of the available NoSQL datastores and stream/historical data processing engines. In addition, it is also necessary to choose either parallel processing engines such as Hadoop or sequential processing once based on the amount of data projected across the crowd sourcing platform [23]. However, it is essential to integrate the data processing aspect with secure blockchain platform to keep away the intruders by imposing penalties in the form of tokens towards every invalid attempt made to gain access.

3. Blockchain Based Consumer Electronics Model

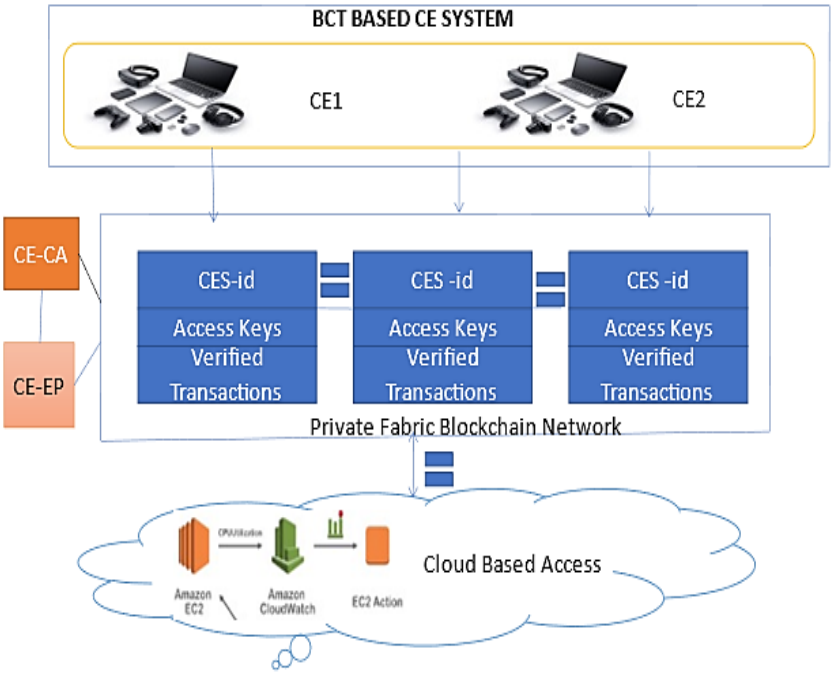

Fig. 3. B2CES Methodology

Blockchain Based Consumer Electronics (CE) Store(B2CES) model is proposed in this work as shown in fig.3 to provide secure access across various consumer electronics stores by using the familiar blockchain technology. In this model, every CE goes through a verification process by the CE-CA, who is the Certification Authority. Once they are marked as verified(V), they can take part in the procurement of various services such as placing orders, buying, selling activities etc. If the identity is verified to be a non-genuine one, then the access to that CE is blocked from gaining entry inside the network. Then, for all the verified CE's, a pair of access keys are assigned by the CE-EP, who is the Endorsing Peer that endorses the transactions as recorded in the CE blocks. Embed these changes in a cryptographic manner inside the code based on key-based access provision facilitated to the authorized users [24].

The B2CES methodology is discussed as follows: If Ti is the transaction cost for a contract Ci under execution, then Ti (i=1to n)<Ci(i=1ton), then

1. Set a counter such that for execution of the same contract (no change in code), the counter does not get incremented. Hence, no Ti.

2. If the code changes, then the counter is incremented, thereby incurring Ti.

3. If the code changes multiple times within a stipulated time frame, then raise an alert to the admin (Ai).

4. If malicious access is found, block (Bi) it immediately.

5. Else send an alert to the user to omit (Oi)multiple code

modifications.

The above-mentioned steps are embedded within a crypto key. This facility makes it efficient to keep track of unwanted user access and reduce the transaction cost. The next algorithm BCE(i) is to carry out the verification and validation process before granting keys to the users to gain access into the system.

Algorithm 1. (Blockchain BCE(i))

Start

1. Verify V[CE(i=1 to n)]
2. If Valid(V)
3. then grant(Ki)
4. Verify V(Ti)
5. If Valid(V)
6. then grant(PkPr)
7. CE(CA) allocate CE(EP)
8. For all CE, CE(EP) repeat steps 1 & 2
9. If Block(Bi) is full, then Cloud (Ci) <- Block(Bi)
10. Only admin(A) can access Cloud (Ci)
11. If !(A), then block access, add to BlockList(U)
12. Repeat steps 3 to 7 for every CE

End

Initially, verify the identity of every Consumer Electronics Store (CES) taking part in the blockchain network. If the identity is valid(V), then grant the corresponding keys (Ki) generated via their digital signatures and hashing as in step 1. Then verify the transactions emitted by the CE $(i = 1\ to\ n)$. If found valid, grant Public and private key pairs (PkPr) to individual blocks. These steps are carried out by the Endorsing Peers (EP) as appointed by the Central CE Authority (CE(CA)) respectively. Once the Block (Bi) is found to exceed its maximum capacity, push data to Cloud (Ci), which is accessible only to the admin (here, CE(CA)). If other unregistered users are trying to gain access, then block the access, add them to the BlockList(U). Repeat these steps for every CE to prevent malicious users into the System.

Algorithm 2. Admin Grant Access Algo (Admin Grantaccess(Ga(i))

Start

1. If Admin(Ai) for each CES(i) where i=1to n responds in time Ti
2. then validate(Epi)
3. Else Block access(Ai)
4. Goto CE(CA)
5. Repeat steps 1 to 4

End

The access to the users should be provided based on their response to the admin within a stipulated time. If the users are not responding within a timeframe fixed in the contracts, the access should be blocked (Ai). This procedure should be repeated for every inactive user or malicious user trying to gain access into the CE system.

4. B2CES Based Results and Discussion

As the nature of data gets complex to secure, it is necessary to identify a suitable platform to implement and deploy the contracts in a cost-effective way. To address this issue, an Ethereum platform is preferred for open data. As an initial phase of the work, implementation is carried out on Ethereum private network using Geth environment. As more than 600 GB space is needed to set up a fully active Geth environment, in this work only a partial one with minimal set of nodes and storage space <16GB was configured onto the local machine. The interaction was carried out via JSON API calls across the nodes. Here, each node is allocated a specific set of permissions and tasks as per which the respective transactions are executed for closed data access respectively. Finally, security issues should be addressed as per the service layer under consideration. Device level layers such as IoT that capture data across a heterogeneous set are at a greater risk of being susceptible to the attackers [25]. Hence, the security algorithms to be developed for this level need to be strengthened by inclusion and amalgamation of various security parameters.

The utility of Ethereum blockchain proves to be efficient when dealing with non-critical data due to the public deployment capability across the internet of nodes. The wallet associated with the network adds the suitability to derive ethers which enable smooth transaction processing, execution, and deployment respectively. However, if the contract is to be modified many times, then it is not a cost-effective mechanism due to the culmination of cost deduction in terms of transaction and gas fee at every modification phase. It is also essential to identify the scope of acceptance for a wide number of user-defined functions [26]. This will also help to keep away intruders or malicious users from participating in network related activities [27].

TABLE 2

BC BASED CONSUMER ELECTRONICS STORE TRANSACTION TIME AND ACCESS TIME ANALYSIS

BC2ES Items	Transaction Time to add items to blocks	Access Key Time generation	Key Verification Time
1	0.23	0.50	0.70
10	0.45	0.65	0.80
50	0.70	0.90	0.90
100	1.50	2.10	3.20
200	2.28	3.50	5.40
300	5.10	6.25	8.50
500	7.12	10.45	12.30

Note: all time units are recorded in seconds for tables

It is identified from table 2 that the emphasis is on the number of items or products recorded onto the nodes rather than the scalable set of nodes. As the number of items increases, the transaction time also increases. There is also a significant increase in the key generation and verification time against the allocation of the number of items onto the nodes respectively. The time taken to perform verification across the nodes is considerably high as compared to the time taken to add the transactions to the blocks and generate the keys as recorded in figure 4 respectively. Each node on Geth is allocated a specific set of permissions and tasks as per which the respective transactions are executed; in the

next phase, the implementation would be developed onto the permissioned fabric.

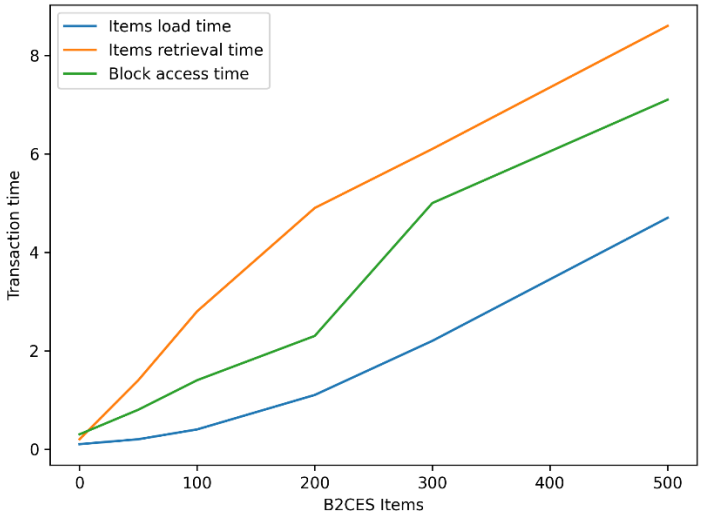

Fig. 4. BC based Consumer Electronics Store Transaction time and Access time Analysis

Table 3. BC Based Consumer Electronics Store Load Time and Retrieval Time Analysis

BC2ES Items	Items load time	Items retrieval time	Block access time
1	0.10	0.38	0.23
10	0.20	0.67	0.45
50	0.30	1.56	0.70
100	0.50	2.89	1.50
200	1.14	4.90	2.28
300	2.27	6.12	5.10
500	4.78	8.60	7.12

As shown in table 3, the time taken to load the items onto the blockchain network increases with the number of items. While the time taken to retrieve the number of items is nearly double the load time, the block access time is an intermediate metric recorded between the load and retrieval times respectively as shown in Figure 5.

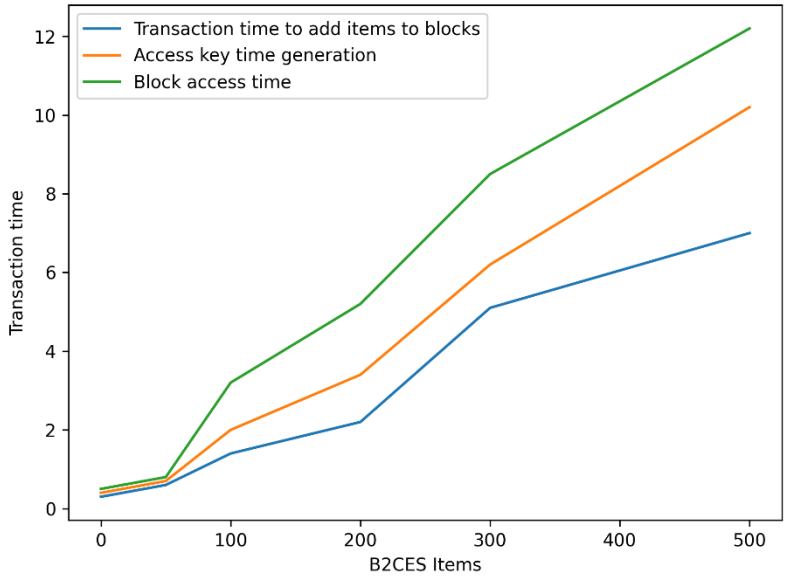

Fig. 5. BC based Consumer Electronics Store Load time and Retrieval time Analysis

At the other end, though there exists a wide set of works in the literature in the direction, a similar work as represented by the authors in [28] emphasized the significance of blockchain in terms of load, retrieval, and block access time respectively. Though there is an improvement in terms of time taken in the proposed BC2ES system as compared to the existing one, the metrics are recorded in seconds as shown in table 4 respectively. In addition, as compared to [32], where the block access time across the nodes in geth environment ranges between 12 sec to 14 sec approximately, the proposed model achieves better results in ranging from 0.23 to 7.12 seconds to access as many as 500 items respectively as shown in table 5. This shows a significant improvement using the proposed approach to deal items access via blockchain network. As a future extension, the ability to deal with scalability in terms of increasing number of stores and items per store as well as time taken to perform various operations across the

blockchain network can be further optimized to milliseconds thereby resulting in a considerable performance improvement. It is also identified from Table 4 that the time taken to retrieve the items is same as the time taken to access any node inside a block respectively. This feature is changing and is recorded low in the proposed system against the number of items maintained onto the blockchain as many as 500.

Table 4. Versus BC2ES Comparative Analysis [28]

BC2ES Items	Existing load time [28]	Proposed Items load time	Existing Items retrieval time[28]	Proposed Items retrieval time	Existing Block access time[28]	Proposed Block access time
1	0.43	0.10	0.56	0.38	0.56	0.23
10	0.45	0.20	0.68	0.67	0.68	0.45
50	0.45	0.30	1.70	1.56	1.70	0.70
100	0.46	0.50	2.95	2.89	2.95	1.50
200	1.25	1.14	5.91	4.90	5.91	2.28
300	3.56	2.27	6.35	6.12	6.35	5.10
500	5.50	4.78	9.29	8.60	9.29	7.12

Table 5. Block Access based comparative analysis

BC2ES Items	Existing Block access time[32]	Proposed Block access time
1	5.56	0.23
10	7.68	0.45
50	10.70	0.70
100	12.00	1.50
200	12.14	2.28
300	13.05	5.10
500	13.87	7.12

The comparative analysis of block access times between the existing and proposed methods reveals from table 5 a significant improvement in performance across all tested scenarios. In the existing method, block access times range from 5.56 to 13.87 for varying block sizes, whereas in the proposed method, these times are notably reduced, ranging from 0.23 to 7.12. Particularly noteworthy is the drastic decrease in access time for larger block sizes, with the proposed method consistently outperforming the existing method. These results underscore the efficiency gains achieved by implementing the proposed approach, demonstrating its potential for enhancing overall system performance and responsiveness in block access operations.

5. Limitations of the Study

While the Blockchain-Based Consumer Electronics Store (B2CES) model demonstrates promising results, several limitations merit consideration. Firstly, the study primarily focuses on transaction times, access times, load times, and retrieval times, neglecting other potential performance metrics that could provide a more comprehensive understanding of the system's functionality. Moreover, the research is confined to a theoretical framework and does not include empirical validation through real-world implementation or user feedback. Another limitation pertains to the scalability of the proposed model. Although the B2CES model shows efficiency gains in block access operations, scalability challenges may arise as the number of stores and items per store increases. Additionally, the study does not address potential security vulnerabilities that could compromise the integrity and confidentiality of consumer data stored on the blockchain network.

Furthermore, the research is conducted within the context of a controlled environment, utilizing a partial Ethereum network with limited storage space. This may not accurately reflect real-world conditions where larger datasets and diverse network configurations are prevalent. Additionally, the study does not explore the energy consumption implications of blockchain technology, an important consideration given the increasing global concerns regarding sustainability. Lastly, the findings of the study are based on a specific implementation of the B2CES model and may not be generalizable to other blockchain-based consumer electronics systems or industries. Further research is needed to evaluate the applicability and effectiveness of the proposed model across different domains and organizational settings.

Directions for Future Research:

1. Explore advanced techniques for enhancing security and privacy of blockchain-based consumer electronics systems.
2. Investigate methods to optimize energy efficiency of blockchain networks, particularly in resource-constrained environments.
3. Extend functionality of blockchain-based systems to support IoT integration, AI applications, and interoperability with other technologies.

6. Conclusion

Consumer Electronics, where one common use is smart homeowners using a variety of devices to efficiently access services. The amount of smart equipment being used in homes to simplify services is rapidly rising. Although having such electronics makes life easier, they also raise questions about security. Consequently, a blockchain platform serves as an appropriate solution to address the issues, ensuring secure access to the services recorded as blocks. Additionally, the availability of a large selection of consensus algorithms to reach a shared understanding among a group of nodes in the block-based network enables people to create secure and adaptable user requirements that adhere to the applications. Therefore, several intelligent and secure blockchain-based case studies for consumer electronics platforms are presented in this work, with a focus on the security attacks that target different consumer electronics products. Different blockchain solutions are also provided to get around these challenges. It is identified from the results that the time taken to load and retrieve the items ranging from 1 to 500 in the proposed Blockchain Based Consumer Electronics Store (B2CES) work is linearly increasing from 0.10 sec to 8.60 secs than a drastic increase ranging from 0.38sec to 9.29secs as identified in the existing

works. In addition, the time taken to access a set of items in a block is also recorded to be as low as 7.12 sec as compared to 9.29 secs invested in accessing a block with 500 items respectively. However, the ability to deal with scalability in terms of increasing number of stores and items per store as well as time taken to perform various operations across the blockchain network can be further optimized to milliseconds thereby resulting in considerable performance improvement.

Acknowledgement: The authors would like to express their sincere gratitude to their respective institutions for providing the necessary facilities and support to carry out this research work. They also thank their colleagues and mentors for their valuable suggestions, technical discussions, and encouragement throughout the course of the study. The authors are grateful to all individuals who contributed directly or indirectly to the successful completion of this work.

Author Contributions: Srinivasarao Goda conceptualized the study, designed the methodology, and supervised the overall research work. Pratap Pachipulusu contributed to the literature review, system design, and experimental analysis. Sakhamuru Amulya was responsible for data collection, implementation, and performance evaluation. Pathan Hussian Basha assisted in result validation, manuscript preparation, and revision. All authors reviewed and approved the final manuscript.

Conflict of Interest: The authors declare no conflict of interest regarding the publication of this paper. This research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Data availability Statement: Data is available on request

Funding: This research received no external funding.

Similarity checked: Yes

References

[1] Ma, J., Lin, S.-Y., Chen, X., Sun, H.-M., Chen, Y.-C., & Wang, H. (2020). A Blockchain-Based Application System for Product Anti-Counterfeiting. IEEE Access, 8, 77642-77652. https://doi.org/10.1109/ACCESS.2020.2972026.

[2] Bai, L., Hu, M., Liu, M., & Wang, J. (2019). BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT. IEEE Access, 7, 58381-58393. https://doi.org/10.1109/ACCESS.2019.2914223.

[3] Sciume, G., Palacios-García, E. J., Gallo, P., Sanseverino, E. R., Vasquez, J. C., & Guerrero, J. M. (2020). Demand Response Service Certification and Customer Baseline Evaluation Using Blockchain Technology. IEEE Access, 8, 139313-139331. https://doi.org/10.1109/ACCESS.2020.3012781.

[4] Mohammed Adam Kunna Azrag, SK Khaza Shareef, Jonardo Ann, & Suraya Masrom. (2023). A Novel Blockchain-based Framework for Enhancing Supply Chain Management. International Journal of Computer Engineering in Research Trends, 10(6), 22–28. https://doi.org/10.22362/ijcert/2023/v10/i06/v10i0604

[5] Liu, D., Alahmadi, A., Ni, J., Lin, X., & Shen, X. (2019). Blockchain-Enabled Data-Sharing Retail Marketing Atop PoS Blockchain. IEEE Transactions on Industrial Informatics, 15(6), 3527-3537. https://doi.org/10.1109/TII.2019.2898900.

[6] Vashistha, N., Hossain, M. M., Shahriar, M. R., Farahmandi, F., Rahman, F., & Tehranipoor, M. M. (2022). eChain: A Blockchain-Enabled Ecosystem for Electronic Device Authenticity Verification. IEEE Transactions on Consumer Electronics, 68(1), 23-37. https://doi.org/10.1109/TCE.2021.3139090.

[7] Lakshmi Sahasra, Thummalapally Anvitha Reddy, & K. Venkatesh Sharma. (2023). Empowering Voting Integrity: An Empirical Study of Blockchain Smart Contracts in Electoral Systems. International Journal of Computer Engineering in Research Trends, 10(11), 37–46. https://doi.org/10.22362/ijcert/2023/v10/i11/v10i115

[8] Islam, M. N., & Kundu, S. (2022). Remote Device Management via Smart Contracts. IEEE Transactions on Consumer Electronics, 68(1), 38-46. https://doi.org/10.1109/TCE.2021.3139584.

[9] Paliokas, I., Tsoniotis, N., Votis, K., & Tzovaras, D. (2019). A Blockchain Platform in Connected Medical-Device Environments: Trustworthy technology to guard against cyberthreats. IEEE Consumer Electronics Magazine, 8(4), 50-55. https://doi.org/10.1109/MCE.2019.2905516.

[10] Su, X., Liu, Y., & Choi, C. (2020). A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions. IEEE Consumer Electronics Magazine, 9(4), 56-66. https://doi.org/10.1109/MCE.2020.2969198.

[11] Xia, P., et al. (2020). Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. In 2020 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-14). https://doi.org/10.1109/eCrime51433.2020.9493255.

[12] Saxena, A., Kumar, D., Singh, B. P., Jatt, B. L., & Kumar, J. S. (2022). Investigating the Charity Funding System using Blockchain Technology. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 877-882). https://doi.org/10.1109/AIC55036.2022.9848986.

[13] Zichichi, M., Contu, M., Ferretti, S., & D'Angelo, G. (2019). LikeStarter: a Smart-contract based Social DAO for Crowdfunding. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 313-318). https://doi.org/10.1109/INFCOMW.2019.8845133.

[14] Jia, A. L., Rao, Y., & Shen, S. (2021). Analyzing and Predicting User Donations in Social Live Video Streaming. In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 1256-1261).

https://doi.org/10.1109/CSCWD49262.2021.9437676 .

[15] Tang, M., & Huang, J. (2021). How Do You Earn Money on Live Streaming Platforms? A Study of Donation-Based Markets. IEEE/ACM Transactions on Networking, 29(4), 1813-1826. https://doi.org/10.1109/TNET.2021.3071488.

[16] Omar Levano-Stella, Jonardo L. Lerios, & Mohamed Remaida. (2023). A Blockchain-based Approach for Securing IoT Devices in Smart Homes. International Journal of Computer Engineering in Research Trends, 10(10), 8–15. https://doi.org/10.22362/ijcert/2023/v10/i10/v10i102

[17] YU, H.-y., DONG, P.-w., & MA, T. (2018). Exploring Donors' Online Charity Adoption Base on Trust on Information Adoption Process. In 2018 International Conference on Management Science and Engineering (ICMSE) (pp. 110-118). https://doi.org/10.1109/ICMSE.2018.8745097.

[18] Saxena, A., Kumar, D., Singh, B. P., Jatt, B. L., & Kumar, J. S. (2022). Investigating the Charity Funding System using Blockchain Technology. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 877-882). https://doi.org/10.1109/AIC55036.2022.9848986.

[19] Salido-Andres, N., et al. (2018). Nonprofit organizations at the crossroads of offline and online fundraising in the digital era: The influence of the volume of target beneficiaries on the success of donation-based crowdfunding through digital platforms. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). https://doi.org/10.23919/CISTI.2018.8399343.

[20] Conrad, C., & Keselj, V. (2016). Predicting Political Donations Using Twitter Hashtags and Character N-Grams. In 2016 IEEE 18th Conference on Business Informatics (CBI) (pp. 1-7). https://doi.org/10.1109/CBI.2016.42.

[21] M.Bhavsingh, K.Samunnisa, & B.Pannalal. (2023). A Blockchain-based Approach for Securing Network Communications in IoT Environments . International Journal of Computer Engineering in Research Trends, 10(10), 37–43. https://doi.org/10.22362/ijcert/2023/v10/i10/v10i106

[22] Saxena, A., Kumar, D., Singh, B. P., Jatt, B. L., & Kumar, J. S. (2022). Investigating the Charity Funding System using Blockchain Technology. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 877-882). https://doi.org/10.1109/AIC55036.2022.9848986.

[23] Zichichi, M., Contu, M., Ferretti, S., & D'Angelo, G. (2019). LikeStarter: a Smart-contract based Social DAO for Crowdfunding. In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 313-318). https://doi.org/10.1109/INFCOMW.2019.8845133.

[24] Jia, A. L., Rao, Y., & Shen, S. (2021). Analyzing and Predicting User Donations in Social Live Video Streaming. In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 1256-1261). https://doi.org/10.1109/CSCWD49262.2021.9437676 .

[25] Tang, M., & Huang, J. (2021). How Do You Earn Money on Live Streaming Platforms? A Study of Donation-Based Markets. IEEE/ACM Transactions on Networking, 29(4), 1813-1826. https://doi.org/10.1109/TNET.2021.3071488.

[26] Alblihed, N., et al. (2022). Developing Food Charity Operations Management System. In 2022 2nd International Conference on Computing and Information Technology (ICCIT) (pp. 93-96). https://doi.org/10.1109/ICCIT52419.2022.9711609.

[27] YU, H.-y., DONG, P.-w., & MA, T. (2018). Exploring Donors' Online Charity Adoption Base on Trust on Information Adoption Process. In 2018 International Conference on Management Science and Engineering (ICMSE) (pp. 110-118). https://doi.org/10.1109/ICMSE.2018.8745097.

[28] Saxena, A., Kumar, D., Singh, B. P., Jatt, B. L., & Kumar, J. S. (2022). Investigating the Charity Funding System using Blockchain Technology. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 877-882). https://doi.org/10.1109/AIC55036.2022.9848986.

[29] Salido-Andres, N., et al. (2018). Nonprofit organizations at the crossroads of offline and online fundraising in the digital era: The influence of the volume of target beneficiaries on the success of donation-based crowdfunding through digital platforms. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). https://doi.org/10.23919/CISTI.2018.8399343.

[30] Ali Vatankhah Barenji, Yaling Zhang, & M Bhavsingh. (2023). A Blockchain-based Framework for Enhancing Privacy and Security in Online Transactions . International Journal of Computer Engineering in Research Trends, 10(11), 1–9. https://doi.org/10.22362/ijcert/2023/v10/i11/v10i111

[31] Zhao, J., Dong, K., & Yu, J. (2014). Recommending funding collaborators with scholar social networks. In 2014 International Conference on Data Science and Advanced Analytics (DSAA) (pp. 122-127). https://doi.org/10.1109/DSAA.2014.7058062.

[32] Dusil, G., & Cerny, D. (2018). The Next Evolution in Funding Innovation. In 2018 International Joint Conference on Neural Networks (IJCNN) (pp. 1-4). https://doi.org/10.1109/IJCNN.2018.8489236.

[33] Kim, H. G., & Kim, S. S. (2016). Utilizing a Distributed Publish/Subscribe System for Connecting Online Shopping Services with Social Funding Projects. In 2016 International Conference on Information Science and Security (ICISS) (pp. 1-2). https://doi.org/10.1109/ICISSEC.2016.7885871.

[34] Saxena, A., Kumar, D., Singh, B. P., Jatt, B. L., & Kumar, J. S. (2022). Investigating the Charity Funding

System using Blockchain Technology. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 877-882). https://doi.org/10.1109/AIC55036.2022.9848986.

[35] Hu, B., Chen, Y., Yu, H., Meng, L., & Duan, Z. (2022). Blockchain-Enabled Data-Sharing Scheme for Consumer IoT Applications. IEEE Consumer Electronics Magazine, 11(2), 77-87. https://doi.org/10.1109/MCE.2021.3066793.

[36] Lamberti, F., Gatteschi, V., Demartini, C., Pelissier, M., Gomez, A., & Santamaria, V. (2018). Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage. IEEE Consumer Electronics Magazine, 7(4), 72-81. https://doi.org/10.1109/MCE.2018.2816247.

[37] Oh, H., Park, S., Choi, J. K., & Noh, S. (2021). Deposit Decision Model for Data Brokers in Distributed Personal Data Markets Using Blockchain. IEEE Access, 9, 114715-114726. https://doi.org/10.1109/ACCESS.2021.3104870.

[38] Sestrem Ochoa, I., Leithardt, V., Calbusch, L., Santana, J., Parreira, W. D., Seman, L., & Zeferino, C. (2021). Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. Applied Sciences, 11(3), 1255. https://doi.org/10.3390/app11031255.

[39] Khan, A. U. R., & Ahmad, R. W. (2022). A Blockchain-Based IoT-Enabled E-Waste Tracking and Tracing System for Smart Cities. IEEE Access, 10, 86256-86269. https://doi.org/10.1109/ACCESS.2022.3198973.

[40] Liu, T., Yuan, Y., & Yu, Z. (2023). An Intelligent Optimization Control Method for Enterprise Cost Under Blockchain Environment. IEEE Access, 11, 3597-3606. https://doi.org/10.1109/ACCESS.2023.3235481.

[41] Lv, Z., Cheng, C., Guerrieri, A., & Fortino, G. (2023). Behavioral Modeling and Prediction in Social Perception and Computing: A Survey. IEEE Transactions on Computational Social Systems, 10(4), 2008-2021. https://doi.org/10.1109/TCSS.2022.3230211.

[42] Mighan, S. N., Misic, J., & Misic, V. B. (2024). Block and Transaction Delivery in Ethereum Network. IEEE Transactions on Network Science and Engineering, 11(1), 926-942. https://doi.org/10.1109/TNSE.2023.3310811.

[43] Ma, L., Liu, X., Li, Y., Zhang, C., Shi, G., & Li, K. (2024). GFBE: A Generalized and Fine-Grained Blockchain Evaluation Framework. IEEE Transactions on Computers, 73(3), 942-955. https://doi.org/10.1109/TC.2024.3349654.

[44] Li, G., Fan, Z.-P., & Wu, X.-Y. (2023). The Choice Strategy of Authentication Technology for Luxury E-Commerce Platforms in the Blockchain Era. IEEE Transactions on Engineering Management, 70(3), 1239-1252. https://doi.org/10.1109/TEM.2021.3076606.