International Journal of Theoretical & Applied Computational Intelligence
https://ijtaci.com

Research Article

A Blockchain-Based Multi-Agent Security Framework for E-Commerce Systems

Mohammed Hasan Ali[1*] and Muhammad Atif Rasheed[2]

[1]Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Najaf, Iraq
[2] Department at UofT: Business Transformation and Program Management
University of Toronto, Canada.
*Crossponding author Mohammed Hasan Ali (email. mohammed.hasan@sadiq.edu.iq)
https://orcid.org/0000-0001-7963-0918
Received: 22/7/2025; Accepted: 05/9/2025; Published: 03/10/2025
https://doi.org/10.65278/IJTACI.2025.15

Abstract: Agent technologies have recently become a vital instrument for electronic communications networks. The utilization of agent technologies in e-commerce networks might overcome the weaknesses in conventional e-commerce, satisfy consumers' intelligence and individualization, and significantly enhance the effectiveness of online transactions. For example, E-commerce systems may employ computer vision to provide upselling possibilities. That is accomplished by going over previous purchases made by clients and immediately proposing comparable goods that people like interesting. Targets multi-agent e-commerce platform construction problems, such as vulnerability with knowledge, unfair transactions, and so on. This article presents a Multi-agent security model for the E-Commerce (MASM-EC) system based on blockchain technologies based on the technological properties of blockchain technologies: decantation and enforcement. Initially, it explains the e-commerce use of agent technologies, clarifying the hidden hazards. Next, the Executive System is proposed from a data storage point of view, transaction data. Furthermore, the methodology of nodes is checked throughout the agent transaction procedure. The experimental results demonstrate that the approach suggested is used for e-commerce multi-agent platforms.

Keywords: Multi-agent; Security model; E-Commerce transactions; Blockchain

1. Introduction

E-commerce is expanding more worldwide and, in recent times, has overturned the quality of thinking and purchasing. The fast evolution of e-commerce, particularly in China, has also substantially influenced productivity expansion [1]. Chinese e-commerce data showed that China's e-commerce activities totaled RMB 19.35 billion, an annual rise of 29.1% in mid-2019. E-commerce has accelerated the retail sector transformation and is currently one of the leading retail channels [2]. It has given additional chances and difficulties, particularly for Small-Medium enterprises (SMEs). On only one side, thanks to the benefits of e-commerce, SMEs can set up their sales outlets without significant initial expenditure on e-commerce networks. On the other hand, in e-commerce, wholesalers face new difficulties [3]. Capital deficiency is likely to arise in e-commerce, a significant challenge many organizations face in managing their retail businesses. One explanation is that the vast audience of retailers contributes to a considerable increase in sales. As a result, increased inventory levels lead to more capital occupied [4]. Secondly, e-commerce accelerates the movement of commodities considerably by removing intermediary connections on the distributing route. The initial joint capital constraint has thus all been transferred to the ultimate retailer [5].

Due to their weak cash flow, this challenge is further widened for SMEs in e-commerce retailing. The inequality in the supply chain also raises the financial strain on small and medium-sized enterprises. SMEs sometimes had to accept adverse terms, such as advanced payments or delivery delays with liability exemptions to acquire supplies, particularly critical enterprises [6]. This mismatch speeds up the work resource deficit of SMEs, which can lead to an increase in corporate risk. Capital scarcity spreads across the whole distribution chain in the long term, particularly in fluctuating environments [7]. So it is not unexpected that the payment of capital shortfalls became a critical and prevalent method. Moreover, as the Internet proliferates, business data grows explosively, and the communication network is increasingly complicated; conventional e-commerce procedures and accompanying technology face new difficulties, and their shortcomings become increasingly evident [8].

Customers cannot examine all online shops, assess relevant data, and decide reasonably. Mobile nodes are an excellent e-commerce option to tackle this issue. Mobile agents can roam over the networks from one server to the next with their portable and autonomous characteristics. Mobile agents do many duties, such as data exploration, company information analysis, user purchasing, and appointments [9]. Of course, agent-based e-commerce solutions, particularly for mobile consumers, are more enticing. It also saves consumers considerable time and substantially cuts transactional costs and time. Therefore, for many purposes, complementary mobile agent technologies were created. Nevertheless, the multi-agent-oriented e-commerce system continually has centralized control and fails to establish absolute equality, justice, and mutual trust. It does not adequately safeguard users' legal rights, dignity, and information assurance. How e-commerce operations are interrupted, and customer data is ensured [10].

This article proposes a blockchain-enabled low-frequency (LF) implementation platform to address such research problems. The aim is to arrange and manage the resources, processes, and choices using agent technologies through the cross-layered framework. The purpose is to link and coordinate with all sorts of agents of LF operations across their life cycles with a hybridization finite-state machine-based intelligent contract. Furthermore, Blockchain is combined with agent technologies to construct a MASM-EC system that offers a trustworthy operating atmosphere to carry out a smart contract more independently and effectively.

The remainder of the article is as follows: The evolution of e-commerce systems is shown in section 2. In section 3, the suggested multi-agent security model for the E-Commerce (MASM-EC) system is built and implemented. The software analysis and performance assessment of the proposed model are covered in Section 4. Finally, the conclusion and future scope are indicated in Section 5.

2. The background of the e-commerce systems

Blockchain technologies corresponded precisely to the demands of e-commerce transformation. The technological and e-commerce blockchain sectors were, first and foremost, decentralized. The intelligent contractual properties of the Blockchain allowed e-commerce customers to trade effectively everywhere. Secondly, the e-commerce sector wants to keep all users and blockchain technologies connected from all domains. The block could accomplish practical cooperative independence; therefore, a third-party confidence method in the Blockchain is not required to fulfill diverse e-commerce emerging market requirements.

In the investigation of blockchains, local and foreign academic establishments were now showing a developing trend. Home research focuses mainly on finance and medicine, which allows for constant learning and electricity. Zhang et al. highlighted the medical instance of Philips to illustrate that patient identification of medical information and personal privacy was performed using blockchain technologies [11]. Li Qing et al. implemented the decentralized storage solution for training recordings and credit institutions using blockchain technologies and supplied an online learning certification authentication protocol [12].

The blockchain technological implementation study showed a hundred blooms and 100 schools of thinking in international research. As far as the e-commerce business was intense, blockchain studies focused on e-commerce innovations. Richard et al. developed a platform based on blockchain technologies for merchants' credit scores and stopped the fake information on the networking score [13]. The blockchain technology in the scoring system was extended by Alexander Schaub etc. The program made the actual internet comment on the security of merchant credentials. This study presented a multi-focal e-commerce platform based on blockchain technologies and the properties of new blockchain technologies such as centralized, complex manipulation, and transparency. Tackle the security issues of the multi-agent e-commerce systems required no intermediary trust mechanisms. Reputation was described as the combination of views that other agents have acquired. It is generally employed to shape the impression and anticipation of the behaviors of anyone based on prior encounters [14]. Reputation, in general, was viewed as a trustworthy indicator, a confidence-building component. A component of this kind was a motivation to conduct well. Therefore, it was a beneficial side benefit in reputable systems that positively impact stock markets.

Since its inception, processes of trust and satisfaction have been seen as essential aspects of multi-agent system (MAS) design to modify competing ideas and choose among viewpoints obtained from various news providers [15]. A line focusing on the construction of reputation systems had just debuted. Although some plans did not cover the combination of reputational information, others were categorized according to news sources, such as first-hand experiences and knowledge from witnesses, which they utilized to generate trust or popularity [16]. As well as the accessibility and precision of reputation calculations, the legitimacy and consistency of this data were critical demands for putting up a credible reputation process.

The security, technical and social methods were three to control reputations. Security-based methods focus exclusively on protecting the reliability of data validity through encryption. Organizational procedures involve a central authoritative body that monitors, supervises, and sanctions the activities of the actors [17]. If hacked, the data is flawed and reputational calculations are manipulated. Finally, social methods imply that agents can imitate other agents' actions and follow the similarities that were not always relevant within human cultures. In addition, the conditions stated above cannot be guaranteed [18].

"Blockchain technology" is a decentralized system that uses encryption algorithms to preserve a shared, unalterable, and accessible record and is based on a specific participation process and consensus algorithm. Data were organized into historically time-marked chunks in cryptographically signed activities transmitted by members [19].

A hash mechanism was performed to the block contents, creating a unique identification block saved in the next block. Possible changes in block contents were confirmed by hacking it again and matching it with the following block identification. Every member replicated the Blockchain and maintained it [20]. Members noticed a fraudulent effort to distort the data held in the registration, thereby ensuring the unchanging of the register. Some blockchains performed arbitrary activities, including blockchain-based, enabling the required functionality to be implemented in addition to these technologies. It differentiated between unauthorized and authorized blockchain networks (public and private). For example, suppose the names of users are either wholly anonymous or faceless. In that case, a platform was unauthorized, so every customer could engage in the consensus procedure and thus add a new piece to the leader [21]. In comparison, the user's authorized blockchain identity and privileges to engage in an agreement were managed by a subscription service (adding to a register and confirming payments).

A blockchain authorization was published if everyone read the leader. Still, preset users only agree and be confidential if the subscription/identification services even control the right to read the record [22]. It was shown to explore and experience all the benefits of the MAS and synergies. The requirement to enhance safety at MAS (e.g., authenticity, access control, origin, transactional assurances, and information security). It could be the best way to improve MAS safety, and specific efforts were already made to merge these two methods. For instance, Ferrer et al. [23] describe how a collection of officers might agree on specific circumstances and record this understanding by integrating peer networking (e.g., agent community) with cryptography methods without requiring an influential. Finally, the scholar examined the possible benefits and limits of blockchain technology integration with MAS using swarm humanoid robots as an illustration.

Bottone et al. [25] developed a mathematical framework to overcome the constraints implied by using standard blockchain technologies in the block-less, fee-less, decentralized ledger technologies used in wireless communication, wearable technology, and cyber-physical platforms [24]. As a result, the verification time was decreased, and specific calculations were avoided. In addition, the system nodes were translated to the components of a collection of nodes (also related to entities). Nevertheless, data traceability was significantly raised if the system's functionality was blockchain-enabled.

Blockchain technology (BCT) safeguarded its archives (leaders) and their information. However, even though the methods listed above demonstrate the synergy between MAS and BCT, there were no reliable, efficient, and accessible design and implementation unresolved: At what level, how can the MAS incorporate blockchain technologies appropriately?

3. The proposed multi-agent security model for the E-Commerce (MASM-EC) system

This article presents a bid-transaction architecture of hierarchically coupled bidders and fiber security operations between distributed generation to conduct the safe transaction among distributed generation and encourage local decentralized renewable energy usage. It comprises essentially three levels: the user level, the agent level, and the layer blockchain. Each layer has the following information.

3.1 User level

The user level in this structure primarily contains consumers, generators of power, and significant grids, and customers are power generators, too, where there is still an excess in fulfilling their requirements when some residents have renewable energy. To complement every participant's information gathering and to sort out every individual need of the customers for a microgrid payment. It suggests implementing in each consumer some sophisticated, intelligent devices, which are mainly utilized for the data on power generation of the consumer, and offer up it to the topmost level to ensure to sort out the procedures of end-users. Each smart gadget has an encrypting component that encodes the data before distribution to protect integrity and confidentiality.

3.2 Agent layer

The conventional power grid uses a centralized control technique and responds according to the single point of the platform's command and judgment. The base station is hard to interpret the customizable needs of various gadgets in the microgrid because of the significant management and operational burden in normal operating mode, which decreases Micronet operation adaptability and limits the increases in the amount. Owing to agents' high autonomous capacity, multi-agent networks can intelligently sense alterations in the field setting and respond flexibly to working demands in the changing environment. Its fundamental structure is that every lower Agent has full cognition and acts independently. Numerous lower-level agents comply with the orders of a higher-level agent to synchronize the entire action with an upper-level Agent. MAS combines the benefits of a distributed system platform with this architecture.

In the model described in this study, the agent layer performs a connected role. This article proposes to utilize hierarchy multi-agent technologies to coordinate the information treatment of the microgrids to adjust to the features of distributed generation units in microgrids and the elements of Blockchain. Each end-user has some agencies, notably Load Agents (LA), Decentralized Generation Agents (DGA), and Grid Agents (GA), that have various functionalities.

The LA requests the Micro-Grid Agent (MGA) while the DGA delivers its state variables. MGA should present the need for purchases and a proper producer bargaining technique to the Respondent's Believed market system. That means that MGA can begin power trading activities using user-specific rules to finish the strategies energy sales process or the method the user buys energy. Upon completion of MGA, both parties operate on the network based on e-payment and keep records of each payment on the Blockchain to guarantee a stable and safe transfer.

3.3 Blockchain level

There is pretty clear coverage and consumers of the local electricity market. Therefore, it is appropriate to provide a permissions model for entering the blockchain system based on trustworthy surroundings. Local power transfers frequently entail vast quantities of small and frequent operations, and hence hardware investments, wastage of mining efforts, and payment confirmation fees are not insignificant. There are insuperable difficulties with Cryptocurrencies. Firstly, the transactional effectiveness is low, and only around seven payments per second can be supported over the whole BCT system. Secondly, there is no assurance of the security of the transactions. Ultimately, it results in a massive waste of assets under the mining method required to establish an agreement. It thus suggested that transactions be used as a renewable transactional platform.

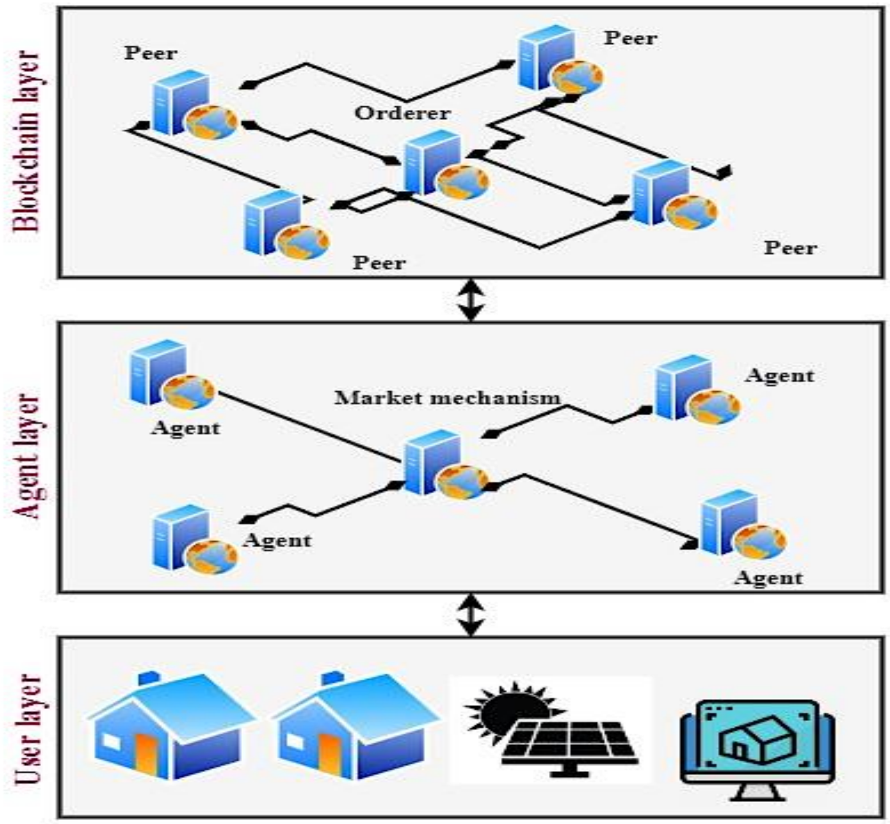

Figure 1: The proposed MASM-EC system's layered architecture

The layered architecture of the proposed MASM-EC system is shown in Figure 1. It has three layers, namely the user layer, agent layer, and blockchain layer. The functions of each layer are explained earlier. In addition, it presents member administration features in comparison to other support. The concept is based on the issuance of certifications by the trust-based organization Confidential Agreement (CA).

Consequently, any member is used the network only after giving the relevant certificate to confirm identification. That allows users to oversee the establishment of a regional microgrid marketplace. In addition, each pair node connecting to the shared book contains a book from the library.

The register comprises two sections: the chain architecture blocking and the storing government records world. The Block Part includes all transactional details, only the query added or subtracted. The State Segment keeps the latest value in the transactional log for all variable's functional dependencies. Therefore, the transactions with Hyperledger Fabric are concluded, and the parameters are recorded to guarantee system security and dependability.

Due to the flexible adaptability of the MAS agent level, additional users and associated facilities are dynamically introduced without modifying other infrastructures, as can be shown through a comprehensive examination of the template presented in this article. Furthermore, the blockchain level is also connected to the networks by the peer nodes accountable for overseeing transaction records. The model offered in the study can therefore be expanded merely to micro-group operations.

Generally, sellers profit more from behavioral economics in a market economy setting. The transactions of other e-commerce salespeople must await the uniform publication of the Grid Trade center in the conventional game contest. The marketplace platform based on blockchain technologies, openness, and information provenance makes competitive pressure a trustworthy, non-central dependency system that reacts rapidly to market knowledge, saves time, and improves knowledge transfer. In other respects, the MGA agent level can rapidly compute the proper bidding technique and enhance the system's effectiveness.

3.4 Multi-agent framework

A multi-agent framework is needed to arrange these agents depending on blockchain actors to meet business requirements in LF. The system design takes into account two issues. First, in light of the simplicity of decentralized creation and use, blockchain agencies' fundamental enabling and general functional needs should be separated and effectively encapsulated. Furthermore, sensitive information should be appropriately segregated among users with potential conflicts.

MAS constructs five essential functions: the intelligent contract systems are accountable for defining, configuring, and executing competent agreements. They connect with the cryptographic protocol product lifecycle. The blockchain services are based on two elements of blockchain administration. On the macro side, the network administration is carried out. The Channel Customization Plan could divide blockchain networks into multi-channel networks among two or more particular agents for privacy and confidentiality data isolation activities. The messaging transport services provide a means for synchronizing message transmission between entities. It uses two types of sending messages: peer-to-peer and public releases.

Peer-to-peer design is developed for commercial logic management agent interactions—the only transmission by an agent to the targeted agency using the Agent's communications language (ACL). Published subscription patterns are utilized for agency blockchain activities since many other agencies generally require an agent's information, notably during the consensus algorithm for decentralized directories. Concerning micro, blockchain companies handle the distributors' ledger specifically.

The transactional service offers agents transaction processes, including the transactions' contents, formats, and concepts. The Agreement Service provides a precise method of consensus. The trade is transacted by the Agent and executed per the selected kind of algorithms according to parameters. Agents are based on the Smart Physical Agents Association standards. The agent administration system manages all agents, such as forming, registering, and removing their agents during the life cycle. Moreover, an index of the agents officially registered in BcMAS is maintained. The database enables agents to publish, find and contact the "yellow page" centralized database.

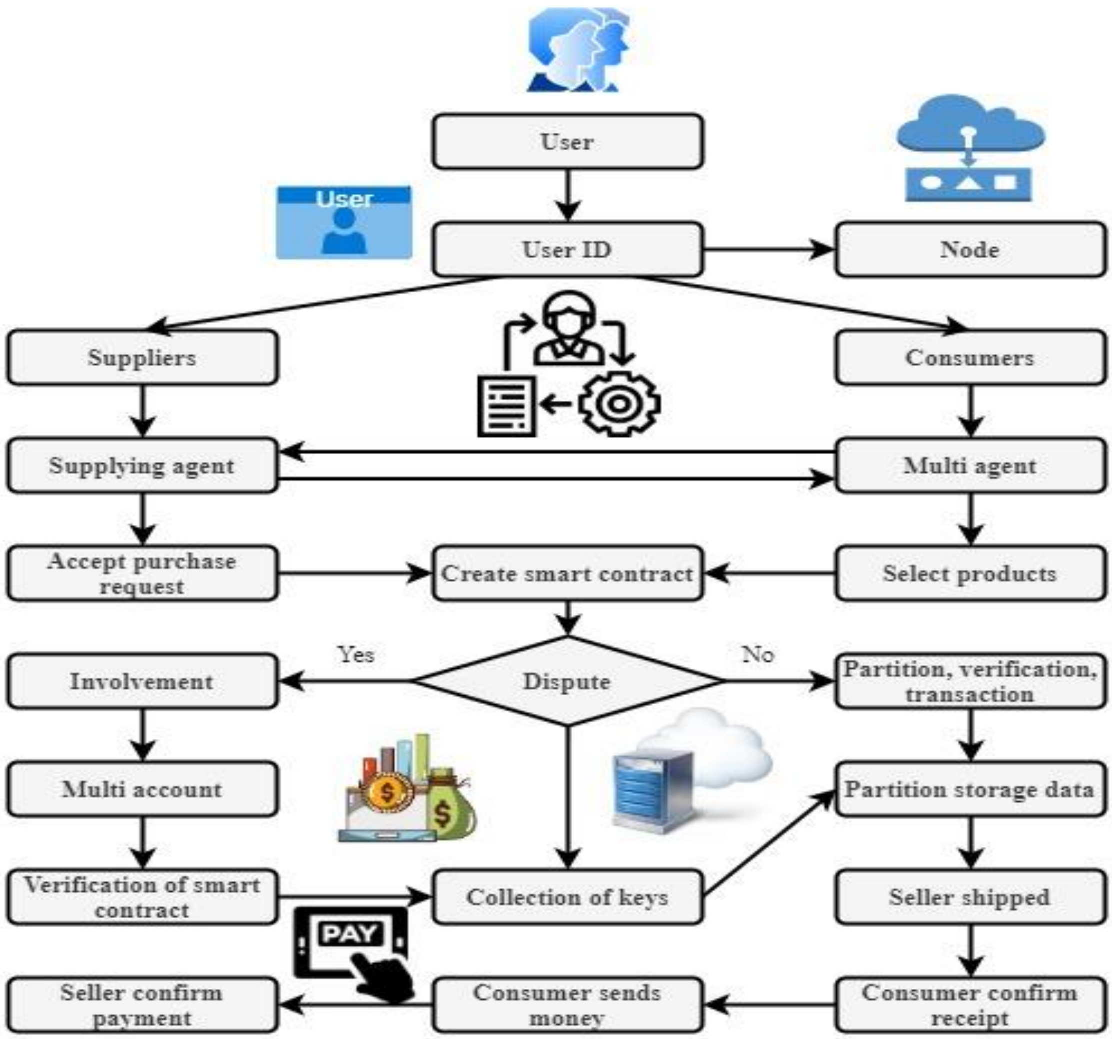

Figure 2: The process flow of the proposed MASM-EC system

The workflow of the proposed MASM-EC system is shown in Figure 2. First, it receives information from the user, such as suppliers and consumers. Both have multiple agents. Then based on the agents from the supplier and consumer side, the intelligent agreement is created. Finally, based on the consumer requirement, the product is shipped, and the payment is received based on the seller can confirm their order. The Agent Participant Solution is intended as a digital identity management service for agencies, and it enables individual agent registration and lays out rules and lists of subscription network access. The agent library provides two kinds of library products. One is the library services of the operator. It produces a driver that poses a considerable challenge for the Agent via compilation based on client kernels and equipment characteristics. The second kind offers an agent-loadable plugin services package for method expansion.

For agents and library durability, the agent library is utilized. It shall be accountable for certificate purchase, renewal, and cancellation. In addition, it is used to provide dealers' certifications of registration and transactions. The interoperable service enables communicating with actors inaccessible for exterior materials content. It uses semantic understanding to autonomously convert protocols, codecs, and commands from communications between heterogeneous distributed applications. On average, MASM-EC can do a blockchain transaction with five stages.

3.5 Proposal for implementation

The applicant representative creates a proposal for implementation and delivers the approach to each supporter necessary in MASM-EC.

3.5.1 Proposal for implementation

Each supporter can perform a brilliant deal based on a suggestion to react to the implementation with a signing autonomously comprising the destination agent.

3.5.2 Proposal for implementation

After many approved execution replies have been obtained, the applications officer inspects those responses. If the test results succeed, a transaction is generated with such answers, and the operation is sent to the ordering agents (OA).

3.5.3 Proposal for implementation

Many application agents accept payments and arrange these applications into blocks.

3.5.4 Proposal for implementation

The API supply blocks for verification to all generic agencies (GA). The blocks verified are placed in the directory.

3.6 Bidding method

Producing companies can optimize their earnings through innovative bids on the energy market. Concerning individual privacy protection, some manufacturers do not like to disclose their correct valuable intelligence. Their bids are defined as a non-cooperative and unfinished gaming procedure. This article follows the following hypotheses before establishing electricity from renewable energy sources with a microgrid. In the energy market trading center, the data of each community is generated, and the costs of other distributed generations are fundamentally the same. They need not know the manufacturing cost of many other microgrid systems except their production costs.

- Distributed generations are not interdependent and cooperative.
- The entire market supply corresponds to need, i.e., the equilibrium of producers and consumers.

Considering that there are N microgrids in the present power marketplace, each microgrid understands only its costs. A microgrid knows how wide varieties of bid microgrids are available based on history and estimates the dispersion of probabilities of rivals through disseminating information. Assuming Microgrid x is cost-effective, and the cost of the micro-grid is denoted in Eq. (1)

$$C(f_x) = p_x f_x^2 + q_x f_x + r_x \tag{1}$$

Where f_x is the x microgrid production, $C(f_x)$ is the overall x, p_x, q_x, and r_x microgrid costs are variables of ongoing cost. The beneficial function of the micro-grid is denoted in Eq. (2)

$$\varphi(f_x) = \mu f_x - \frac{C(f_x)}{x} \tag{2}$$

Where μ is the current electricity cost, microgrid x is considered to have several kinds, and every kind relates to a cost-production process $C(f_x)$. Here, $f_x$represents the function of the input. Indicated to bring together the risk dispersion is the forecast of the likelihood of other microgrids closer to the actual possibility and expressed in Eq. (3)

$$f_{xy}^{pq} = f\left(C_y^q | C_x^p\right) = \frac{f\left(C_y^q\right) f\left(\frac{C_y^q}{C_x^p}\right)}{f\left(C_x^p\right)} \tag{3}$$

f_{xy}^{pq} indicates a likelihood condition. The possibility under microscale y type m cost feature is re-evaluated whenever the differential equation of type n is chosen for microscale x. $f\left(C_y^q\right)$ indicates the last chance of picking the type q objective functions of microgrid y. The likelihood function of $f\left(C_y^q | C_x^p\right)$ is calculated using previous transaction information. For example, taking microgrid 0, allowing the functional form specified to be type 1, the cost pattern is defined in Eq. (4)

$$C(f_0) = p_0 f_0^2 + q_0 f_0 + r_0 \tag{4}$$

p_0, q_0, and r_0 microgrid costs are variables of ongoing cost for the zeroth microgrid. The input function of the micro-grid position is denoted f_0. Then the cost of the next micro-grid is denoted in Eq. (5)

$$\widehat{C(f_0)} = \sum_{k=0}^{n} p_x^k C_x^k (f_x) \tag{5}$$

The cost function of the micro-grid x at a kth time is denoted as C_x^k, the input function is denoted f_x, the transactional security level is denoted p_x^k.

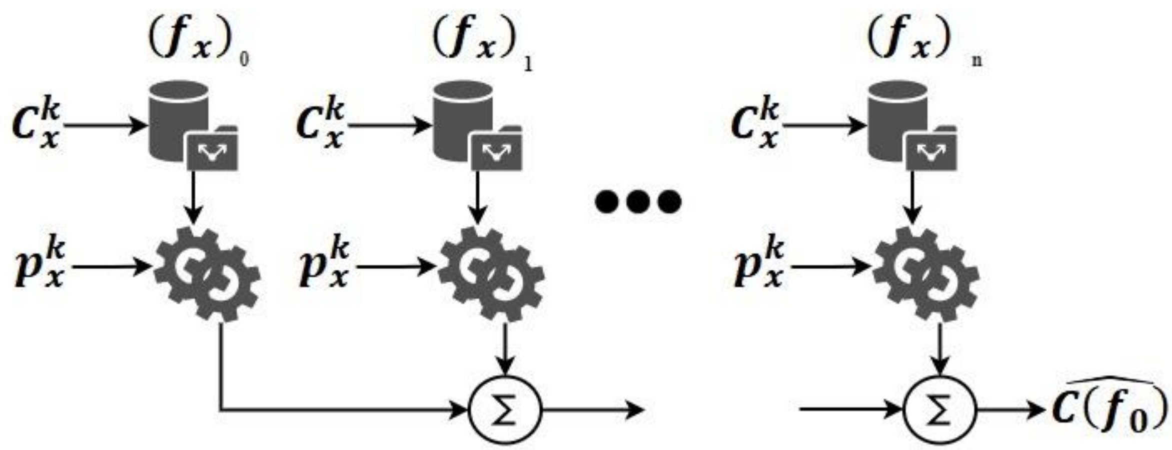

Figure 3: Image-based depiction of $\widehat{C(f_0)}$

Figure 3 is a visual illustration of the expression $\widehat{C(f_0)}$. It employs the benefit-cost analysis, input-output analysis, and safety level to calculate the cost. The simulation has transformed from a biased information gaming to a comprehensive information model based on the Harsanyi transition. The Nash balance is utilized to solve this complete data game. The benefit function of the network x is denoted in Eq. (6):

$$\varphi(f_x) = \mu f_x - \sum_{k=0}^{n} p_x^k C_x^k (f_x) = \mu f_x - \widehat{p_x} f_x^2 + \widehat{q_x} f_x + \widehat{r_x} \tag{6}$$

The cost function is denoted as C_x^k, the input function is denoted f_x, the transactional security level is denoted p_x^k. $\hat{p}_x$, $\hat{q}_x$, and $\hat{r}_x$ microgrid costs are variables of ongoing cost. μ is the cost of power. The differential function of the beneficial process is denoted in Eq. (7)

$$\frac{d\varphi(f_x)}{df_x} = \mu - [2p_0 f_0 + q_0] \tag{7}$$

The micro-grid variables are denoted p_0 and q_0. The cost of unit power is indicated μ. The symbol indicates the input function f_0. according to supply-and-demand balancing assumptions, the overall output E of all distributed generation is defined by the time forecast of the electricity markets. The total energy is denoted in Eq. (8)

$$E = f_0 + f_1 + \cdots + f_{M-1} \tag{8}$$

The incoming data function is denoted f_x. The estimation of the other electricity generation parameters for the microgrid 0 gains and its optimal biding power is denoted in Eq. (9)

$$f_0 = E + \frac{\sum_{k=1}^{M-1} \frac{\widehat{q_x}}{2\widehat{p_x}}}{1+\sum_{k=1}^{M-1} \frac{p_0}{p_k}} \tag{9}$$

$\hat{p}_x$, $\hat{q}_x$, and $\hat{r}_x$ microgrid costs are variables of ongoing cost. The variable of micro-grid 0 is denoted p_0. The total energy is denoted E. The anticipated value of the microgrid 0's variable costs value may be determined using the objective functions. The cost of the micro-grid 0 is represented in Eq. (10)

$$\mu_0 = \mu = \frac{dC(f_0)}{df_0} = 2p_0 f_0 + q_0 \tag{10}$$

Therefore, μ_0, f_0 is the optimal microgrid 0 pricing model. The cost function is denoted μ. The variable of micro-grid 0 is denoted p_0 and q_0.

3.7 Electronic trade simulation model

It proposes a multi-agent electronic trading system using Blockchain and comprises three enterprises: user, email, and network. It consists of two. The development of e-commerce platforms based on Blockchain is shown in Figure 4.

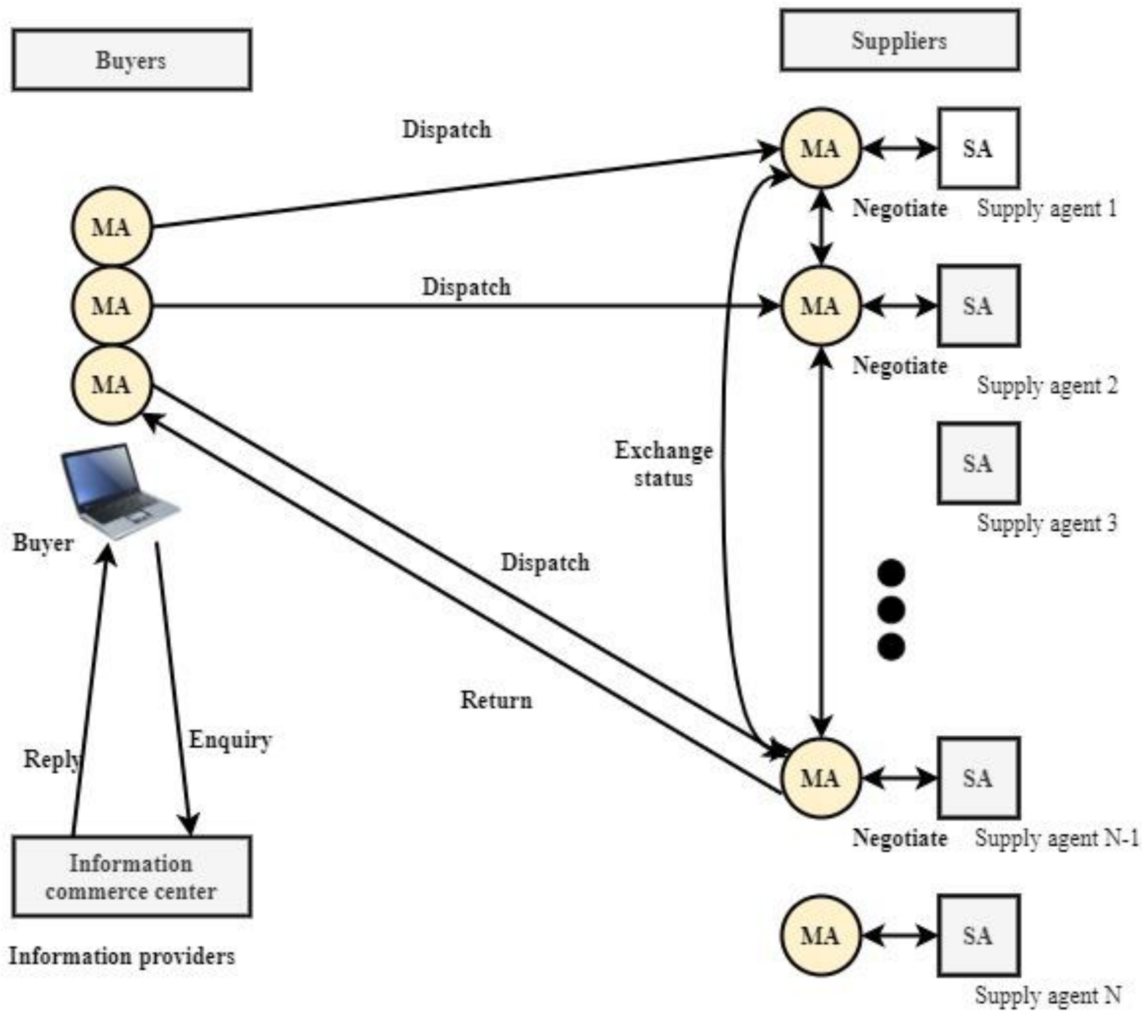

Figure 4: The developmental architecture of the Blockchain-based e-commerce platform

If it sells items on the system, it needs to establish an agent providing a product's price, minimum, number, and more comprehensive details. For example, suppose the purchaser seeks quotations for specific products. In that case, the inquiry is transmitted to the provider part of the center, which replies to the purchaser's list of provider web pages. The trade finances several buyer representatives and sends every Agent to every site on the list. The customer agent collects the quotation from each site provider's Agent and chooses the dealer based on comparison shopping.

Upon picking the chosen goods, the customer can then discuss the pricing, volume, and shipping method with the selling agent. The e-commerce platform creates a consensus protocol based on the purchaser and the purchaser's cryptographic certificates until the agreement is entered. Then, the intelligent contract is submitted to the relevant product characteristic block for validation. If all units are properly checked, they can be sent under the specified terms and conditions. When the purchaser receives the items and confirmation is valid, electronic money is paid directly from the location of the cryptographically signed accounts of the purchaser to the company account. All data is captured from the transaction in the Blockchain flowing node. If sellers and buyers disagree with the purchase, they can have a notary with the other third party to address the matter.

The e-commerce system has created a repute points system for every customer, which allows every user to receive feedback anonymously on the current state of affairs of users transacted with them to maintain the impartiality and reliability of officials. The more awards the digital money has for the customers with more significant points, the better the trustworthiness of the notarized. However, if the notarized is deemed misused by other customers and is genuine, it will be banned. The more awards the signer will have. And levy a very hefty fine. The registrar of each transaction should be selected jointly by the purchaser or the vendor to avoid circumstances in which the registrar favors either party.

In the event of disagreements over the value of the transaction, the notary shall check the software application and establish a multi-signature virtual currency account. Each has a secret key for the registrar and the purchaser. It is only by agreeing to gather all three personal accounts. Then, following the contractual conditions, the purchaser transfers the virtual money to the multi-signature account. If the seller accepts the buyer's payment notification, he delivers the items, and the buyer obtains information about shipping the goods. After confirming the supplier invoice, the purchaser immediately processes the payments from the multi-signed account to the vendor.

4. Software analysis and performance evaluation

An empirical case study to show its associated technologies will be undertaken to validate the suggested MASM-EC system to assist the LF deployment of E-commerce capital-constrained SMEs. The first is to outline the present operational problems and explain and construct the testing situation. Then, the MASM-EC system working prototype is further improved and deployed in inspection and assessment to enable a flexible inventory commitment model. In conclusion, this exploratory, descriptive study is summarised by comparisons and commentary.

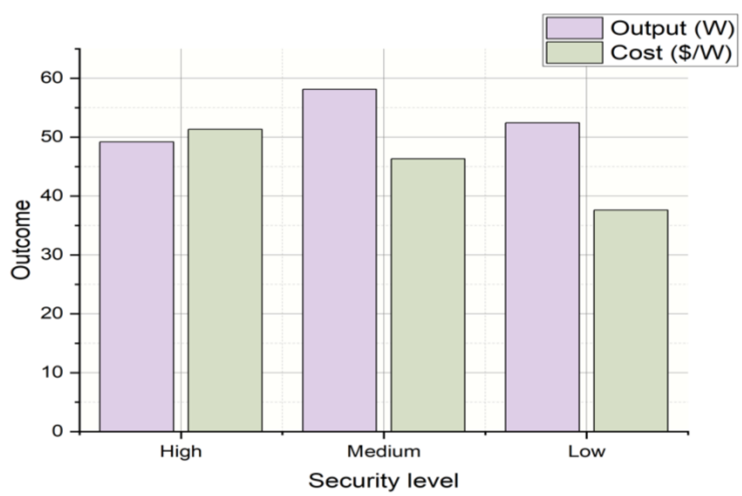

Figure 5(a): Analysis of simulation results using the existing SVM model

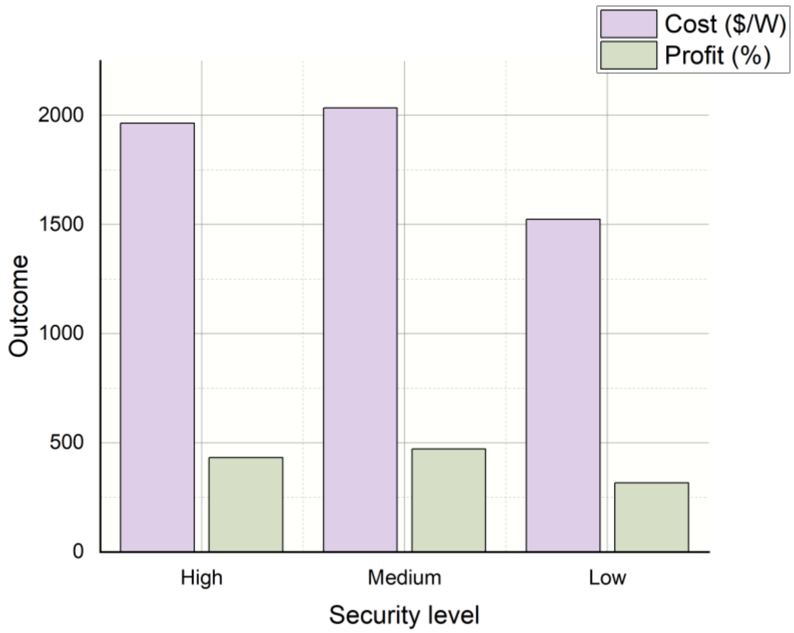

Figure 5(b): Analysis of the proposed MASM-EC system's simulations

Analyzing the results of simulations using the current SVM model and the proposed MASM-EC system are illustrated in Figures 5(a) and 5(b). the different security levels are considered for the simulation analysis. The cost function and the profit of each security level, both the current and planned MASM-EC system, are studied. The result shows the proposed MASM-EC system utilizes significantly less power with the help of simpler architecture and produces a higher security level with the help of Blockchain architecture. As the security level increases, the respective cost also increases.

Table 1: Transaction throughput analysis of the proposed MASM-EC system

Block size (B)	4 agents (texts/sec)	8 agents (texts/sec)
200	120	167
400	248	298
600	532	694
800	687	997
1000	982	1865
3000	1658	2987
6000	2154	3984
10000	6782	8274

An evaluation of the MASM-EC system's transaction throughput is shown in Table 1. In need to do the simulation analysis, the block size of the blockchain architecture from a minimum of 200 bytes to a maximum of 10000 bytes. The respective throughput for the four and eight agents is analyzed and tabulated. As the block size increases, at the same time, the server can send more data, so the system performance improves in terms of higher throughput. In addition, system throughput grows in proportion to the number of agents.

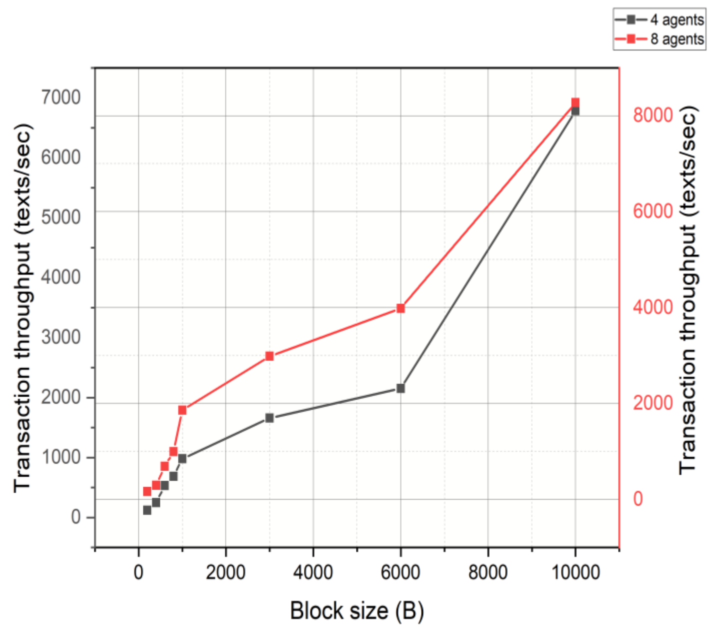

Figure 6(a): Throughput analysis of the proposed MASM-EC system

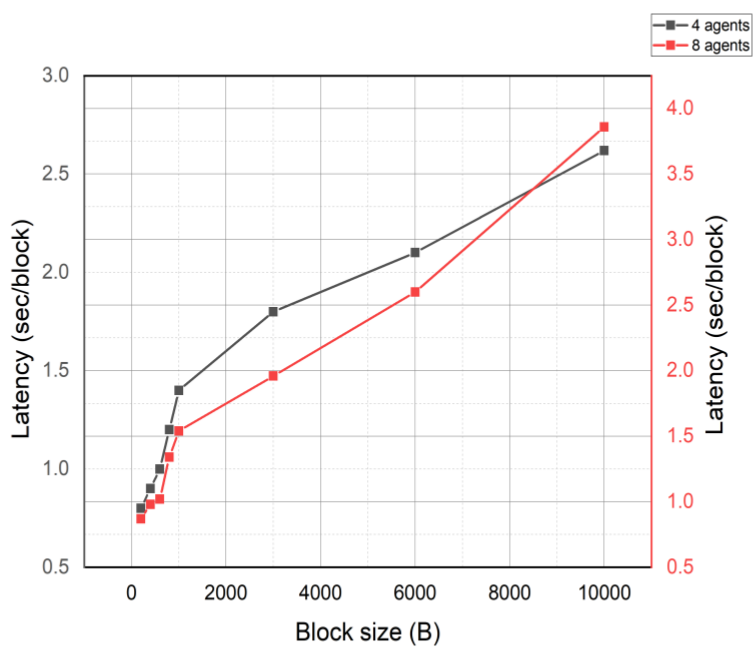

Figure 6(b): Evaluating the MASM-EC system's projected latency

The throughput analysis and latency analysis of the proposed MASM-EC system are shown in Figures 6(a) and 6(b). the simulation analysis of the suggested MASM-EC system is done by varying the Blockchain's block size. The simulation outcomes, such as throughput and latency of the proposed MASM-EC system, analyze 4 and 8 agents. As the block size increases, the respective throughput and latency increase. The throughput increases because the same number of blocks contains more information, and due to each block's larger size, the system's end-to-end latency increases.

Table 2: Analyzing the accuracy and reliability of the proposed MASM-EC system

Block size (B)	4 agents (%)	8 agents (%)
200	86	88
400	87	92
600	89	94
800	91	95
1000	92	96
3000	93	97
6000	94	98
10000	97	98

Table 2 shows an evaluation of the MASM-EC system's precision. The proposed MASM-EC system's block size is examined for 4 and 8 agents, with the accuracy data for each tallied totaled. The suggested MASM-EC system's accuracy improves as the block size grows. This is because when the block size increases, the Block chain has higher security algorithms and a higher data rate. Concerning the number of agents increases, the Agent enhances the more increased connectivity and security level, which results in higher performance of the proposed MASM-EC system. The suggested MASM-EC system's accuracy and precision analyses are shown in Figures 7(a) and 7(b), respectively. The proposed MASM-EC system's simulation analysis is examined. The simulation results are studied and shown, including the suggested MASM-EC system's accuracy and precision with block size. The block size grows, and the proposed MASM-EC system outcome also increases. The proposed MASM-EC system, with the help of Blockchain and the multi-agent model, enhances its performance of the proposed MASM-EC system.

In the proposed MASM-EC, the system is developed, tested, and assessed in this stage. The simulation results, such as accuracy and precision, are evaluated for the proposed MASM-EC system and compared to the current models. The results exhibit the better performance of the proposed MASM-EC system.

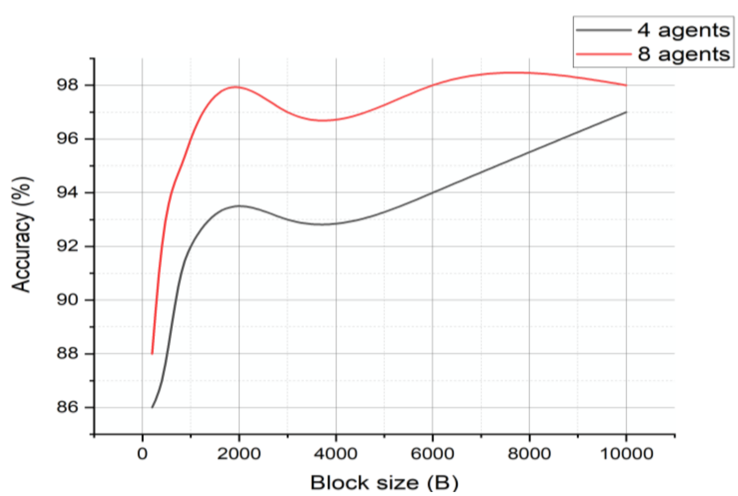

Figure 7(a): Analysis of the proposed MASM-EC system's accuracy

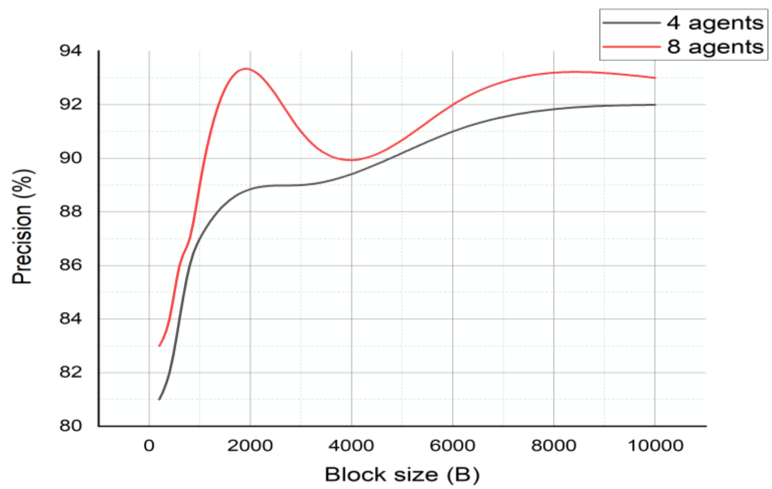

Figure 7(b): Analysis of the proposed MASM-EC system with great precision

5. Conclusion and future scope

This article presents a Multi-agent security model for the E-Commerce (MASM-EC) system based on blockchain technologies. This technology innovation is mainly apparent in the use of decentralized storage devices. The system validation node accomplishes data storage using a consensus technique and utilizes double SHA256. Hashing is coupled to process the transactional data using the encrypting method. Avoid tampering with the secure and trusted trading procedure to ensure the legitimacy of transactional data. Simulation analysis and verification of the leading technology and key algorithms are included in this technique. The test findings demonstrate that blockchain technologies efficiently resolve security issues in e-commerce platforms with many agents.

This article contains several deficiencies in the method. The method will be less effective in attaining total decentralization. For instance, a lot of data must be stored superfluously in every dispersed node, which covers a vast storage area and leads to inefficiencies in the query and validation of the data. A "partial decentralization" or "multi-centered" networking architecture can be created to provide data protection and significantly increase the process's effectiveness. There is also a security concern with blockchain data. This research utilizes a better method for the service agreement. Even though the security algorithm includes the transaction signature authentication protocol, data security is much enhanced, yet the possibility remains of this safety hazard. Consequently, additional study and development are necessary for the protection and efficacy of the consensus process.

Funding: No specific funding received for this research.

Data Availability: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: No conflict of interest is stated by the author.

Authors contributions: Conceptualization: MHA, MAR; methodology: MHA, MAR validation: MHA; writing—original draft preparation, MHA, MAR; writing—review and editing: MHA, MAR; visualization: MHA, MAR; supervision: MHA; project administration: MHA; funding: MAR; The authors had approved the final version.

References

[1] Nguyen, N., Liu, B., Pham, V., et al., (2018). "An efficient minimum-latency collision-free scheduling algorithm for data aggregation in wireless sensor networks". *IEEE Systems Journal*, 12(3), 2214-2225.

[2] Sundarasekar, R., Mohamed Shakeel, P., Baskar, S., et al., (2019). "Adaptive energy aware quality of service for reliable data transfer in under water acoustic sensor networks". *IEEE Access*, 7, 80093-80103.

[3] Vatankhah Barenji, R. (2022). "A blockchain technology based trust system for cloud manufacturing". *Journal of Intelligent Manufacturing*, 33(5), 1451-1465.

[4] Karuppusamy, P., Perikos, I., Shi, F., et al., (2020). "Sustainable communication networks and application". *Lecture Notes on Data Engineering and Communications Technologies*, 65-72.

[5] Nasir, S., Bilal, M., and Khalidi, H. (2025). "Detection and classification of skin cancer by using CNN-enabled cloud storage data access control algorithm based on blockchain technology". *International Journal of Theoretical & Applied Computational Intelligence, 2025*, 145–169.

[6] Gao, J., Wang, H., and Shen, H. (2022). "Task failure prediction in cloud data centers using deep learning". *IEEE Transactions on Services Computing*, 15(3), 1411-1422.

[7] Aggarwal, S., Chaudhary, R., Aujla, G. S., et al., (2019). "Blockchain for smart communities: Applications, challenges and opportunities". *Journal of Network and Computer Applications*, 144, 13-48.

[8] Gheisari, M., Najafabadi, H. E., Alzubi, J. A., et al., (2021). "OBPP: An ontology-based framework for privacy-preserving in iot-based smart city". *Future Generation Computer Systems*, 123, 1-13.

[9] Manogaran, G., and Lopez, D. (2018). "Health data analytics using scalable logistic regression with stochastic gradient descent". *International Journal of Advanced Intelligence Paradigms*, 10(1/2), 118.

[10] Lohmer, J., and Lasch, R. (2020). "Blockchain in operations management and manufacturing: Potential and barriers". *Computers & Industrial Engineering*, 149, 106789.

[11] Yang, A., Li, Y., Liu, C., et al., (2019). "Research on logistics supply chain of iron and steel enterprises based on block chain technology". *Future Generation Computer Systems*, 101, 635-645.

[12] Shi, N., Tan, L., Yang, C., et al., (2021). "BACS: A blockchain-based access control scheme in distributed internet of things". *Peer-to-peer Networking and Applications*, 14(5), 2585-2599.

[13] Darwish, M. A., Yafi, E., Al Ghamdi, M. A., et al., (2020). "Decentralizing privacy implementation at cloud storage using blockchain-based hybrid algorithm". *Arabian Journal for Science and Engineering*, 45(4), 3369-3378.

[14] Pinna, A., and Ibba, S., "A blockchain-based decentralized system for proper handling of temporary employment contracts", *Advances in Intelligent Systems and Computing*, Cham: Springer International Publishing, 1231-1243, (2019).

[15] Salih, H. S., Ali, M. H., Khan, et al., (2025). "IoT-enabled cloud storage data access control model based on blockchain technology". *International Journal of Theoretical & Applied Computational Intelligence*, 125-144.

[16] Yousaf, K., Mehmood, Z., Saba, T., et al., (2019). "Mobile-health applications for the efficient delivery of health care facility to people with dementia (pwd) and support to their carers: A survey". *Biomed Research International*, 2019, 1-26.

[17] Liu, S., Dai, Y., Cai, Z., et al., (2021). "Construction of double-precision wisdom teaching framework based on blockchain technology in cloud platform". *IEEE Access*, 9, 11823-11834.

[18] Hamidi, H., and Kamankesh, A. (2018). "An approach to intelligent traffic management system using a multi-agent system". *International Journal of Intelligent Transportation Systems Research*, 16(2), 112-124.

[19] Alqahtani, F., Al-Makhadmeh, Z., Tolba, A., et al., (2020). "TBM: A trust-based monitoring security scheme to improve the service authentication in the internet of things communications". *Computer Communications*, 150, 216-225.

[20] Alsamhi, S. H., and Lee, B. (2021). "Blockchain-empowered multi-robot collaboration to fight covid-19 and future pandemics". *IEEE Access*, 9, 44173-44197.

[21] Reebadiya, D., Rathod, T., Gupta, R., et al., (2021). "Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5G networks". *Peer-to-peer Networking and Applications*, 14(5), 2757-2774.

[22] Li, W., Cao, M., Wang, Y., et al., (2020). "Mining pool game model and Nash equilibrium analysis for pow-based blockchain networks". *IEEE Access*, 8, 101049-101060.

[23] Zhu, Z., Qi, G., Zheng, M., et al., (2020). "Blockchain based consensus checking in decentralized cloud storage". *Simulation Modelling Practice and Theory*, 102, 101987.

[24] Banyal, S., Amartya, and Sharma, D. K., "Security vulnerabilities, challenges, and schemes in IoT-enabled technologies", *Blockchain Technology for Data Privacy Management*, First edition. | Boca Raton: CRC Press, [2021] | Series: Advances in intelligent decision-making, systems engineering, and project management: CRC Press, 81-108, (2021).

[25] Wang, Y., Su, Z., Zhang, N., et al., (2021). "Learning in the air: secure federated learning for UAV-assisted crowdsensing". *IEEE Transactions on Network Science and Engineering*, 8(2), 1055-1069.