



# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 6, June 2025**

# Blockchain-Based Secure Payment Gateway for E-Commerce Websites

Prabavathi S, Ponmayil R

Student, Department of Master of Computer Applications, Vivekanandha Institute of Information and Management  
Studies, Tiruchengode, Tamil Nadu, India

Assistant Professor, Department of MCA, Vivekanandha Institute of Information and Management Studies,  
Tiruchengode, Tamil Nadu, India

**ABSTRACT:** The purchasing and selling of goods and services using electronic platforms, primarily the internet, is referred to as e-commerce. Efficient and secure online payment systems have emerged as a key component of e-commerce success as the global digital marketplace keeps growing. Conventional e-commerce payment methods mainly depend on third-party services like PayPal or Stripe, as well as centralized gateways like credit/debit cards and net banking. However, there are a number of serious problems with the payment gateways that are currently in use. Because they are centralized, they are vulnerable to identity theft, fraud, data breaches, and cyber attacks. Delays in settlements, high transaction costs, and a lack of transparency all work against user confidence and corporate effectiveness. This project suggests a Block chain-based Secure Payment Gateway for E-Commerce Websites in order to address these issues. By utilizing decentralized block chain technology, it seeks to completely transform the payment environment. By facilitating peer-to-peer transactions that are safely documented on a distributed ledger that is impenetrable to tampering, the suggested method does away with middlemen. It uses smart contracts to automate real-time settlement, escrow management, and payment authorization, guaranteeing transaction efficiency, transparency, and immutability. The gateway uses cryptographic verification to guarantee data integrity and public-private key encryption to facilitate safe user authentication. It has user-friendly interfaces for both consumers and merchants, and it can be easily integrated into current e-commerce platforms. Through the use of blockchain, the system offers a transparent audit trail, speeds up payment processing, lowers transaction costs, and decreases fraud risks. This creative strategy fosters global accessibility and confidence in digital commerce while also improving the security and dependability of online payments.

**KEYWORDS:** Blockchain, Decentralization, Security, Payment, E-commerce.

## I. INTRODUCTION

At present, e-commerce, finance, energy and other fields are developing rapidly, and new technologies are changing with each passing day. In traditional e-commerce, user information leakage risk events occur from time to time. How to use blockchain technology to improve the security of e-commerce systems is an urgent need. As the scale of ecommerce cross-border trade continues to increase, the volume of cross-border payment is rising. In the current crossborder payment process, each transaction needs to be transmitted between multiple organizations. There are problems such as high intermediate costs, low payment efficiency, high membership threshold, and centralized security risks. Traditional ecommerce transactions have their records in a centralized organization, which is inefficient, costly and opaque. The blockchain distributed ledger guarantees the fairness and authenticity of the transaction, and avoids the possibility of transaction being tampered. The advantages of blockchain-based applications are optimizing business processes, reducing operating costs, and improving synergy efficiency. These advantages have been gradually reflected in financial services and supply chain management. Blockchain-based financial asset rights trading and circulation drive the development of financial markets, financial instruments, financial intermediation, and financial system. The payment clearing system is the basic support of economic and financial activities. And the payment clearing process is a typical multi-center scene, which is highly matched with the blockchain characteristics.



## II. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Background E-commerce, or electronic commerce, refers to the buying and selling of goods and services over the internet. With the widespread adoption of internet technologies, e-commerce has witnessed tremendous growth, transforming the way businesses operate and consumers shop. One critical aspect of e-commerce is the payment system, which enables secure and convenient financial transactions between buyers and sellers in the online marketplace. Traditionally, e-commerce payments have relied on traditional payment methods such as credit cards, debit cards, bank transfers, and cash on delivery. While these methods have served as the foundation for online transactions, they come with various limitations, including security vulnerabilities, high transaction fees, slow settlement times, and geographical restrictions. These limitations have prompted the exploration of alternative payment systems, including those based on block chain technology.

### Three types of block chain

- **Public block chain.**

A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of crypto currencies run on a public block chain that is governed by rules or consensus algorithms.

- **Permission or private block chain.**

A private, or permission, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permission blockchain.

- **Federated or consortium blockchain.**

A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

## III. LITERATURE SURVEY

One of the most important transactional channels nowadays is e-commerce. E-commerce deals encompass all three of the public and private sectors. Based on a range of application scenarios, many e-commerce models have been developed. The most common variations are business-to-business (B2B) [5], business-to-customer (B2C)[6], customer-to-customer (C2C)[7], online-to-offline (O2O)[8], and government-to business (G2B)[9]. The most prevalent problems with ecommerce models include the following:

The security of the personal information of the millions of users of e-commerce platforms must be ensured. We routinely learn about cyber-security issues involving breaches or exposures of private consumer data to unintended recipients, who then use it inappropriately. Breach of data integrity and security has repeatedly had devastating results. Therefore, e-commerce websites must have total control over the security of user-sensitive information, such as personal data and related financial data. When providing their private bank account information and other data on a reliable e-commerce site, customers should not worry about hackers stealing their personal information. Therefore, to protect user-sensitive data from hackers, these websites must make use of advanced data encryption technology. Another simple yet essential component of an ecommerce website that controls logistics is supply chain management (SCM). SCM is a crucial component of every organization, whether it be in agriculture, online food delivery, or even an e-commerce platform. From the producer, via the wholesaler, the retailer, and ultimately the eventual consumer, a thing or commodity must travel a long way. The product must first overcome a large number of obstacles along the whole supply chain, including subpar raw materials, sluggish production, poor vendor communication, problems with payment processing, and many, many more before it can ultimately reach its final destination, the client. An efficient payment transaction ledger is a must for every e-commerce effort. To keep a history of each minor or big occurrence during the process, countless transactions that must be securely documented in ledgers or account books [10] are just a few instances. These interactions cover recording client orders, collecting payment information, following an order's progress via the logistics chain, sending the goods to the consumer, returning them for a refund, etc. Blocks, which can be collections of data packages that generally include multitudinous deals, are the simple structure blocks of a block chain. With every new block, the block chain, which serves as a radical report of every sale, expands. Blocks can be demonstrated by using the network using cryptographic strategies. each block also contains the deals, a timestamp, the

hash price of the block that got then before it (the "parent"), and a nonce, which is a arbitrary range used to validate the hash. The integrity of the chain as a total is assured with the aid of this idea.

#### IV. EXISTING SYSTEM

To protect online transactions and build trust among users, traditional e-commerce platforms and payment gateways implement a range of **security measures and protocols**. These methods aim to safeguard sensitive customer information, prevent fraud, and ensure the confidentiality and integrity of payments.

- **SSL/TLS Encryption**

Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocols used to establish a secure connection between the user's browser and the e-commerce server. These protocols encrypt sensitive information such as credit card details and login credentials during transmission, thereby preventing unauthorized access or interception by attackers. Almost all modern e-commerce websites implement HTTPS (SSL-enabled URLs) to ensure secure data transfer.

- **PCI-DSS Compliance**

The Payment Card Industry Data Security Standard (PCI-DSS) is a globally recognized set of security standards established to protect cardholder information. Payment gateways and e-commerce platforms are required to comply with PCI-DSS to ensure secure handling of credit and debit card data. Compliance includes secure storage, encryption, access control, and regular monitoring of financial transactions.

- **Two-Factor Authentication (2FA)**

Two-Factor Authentication adds an additional layer of security by requiring users to provide two types of credentials to complete a transaction. Typically, this involves something the user knows (password or PIN) and something the user possesses (a one-time password sent via SMS or generated by an authentication app). 2FA significantly reduces the risk of unauthorized access due to stolen passwords or phishing attacks.

- **Tokenization**

Tokenization is a method of replacing sensitive card information with a unique token that has no exploitable value. These tokens are used during transactions in place of the actual card number, which is securely stored in a centralized token vault. This technique helps prevent card data theft, as the actual card details are never exposed during the transaction.

- **End-to-End Encryption (E2EE)**

End-to-End Encryption protects data throughout the transaction cycle—from the point it is entered by the user to the point it is received by the payment processor. With E2EE, even if the data is intercepted during transit, it remains unreadable to attackers. This method ensures that sensitive information such as bank details and personal data remain confidential at all times.

- **Fraud Detection and Risk Management**

Modern payment gateways incorporate advanced fraud detection mechanisms powered by artificial intelligence and machine learning. These systems analyze transaction patterns in real time, identify anomalies, and flag or block suspicious activities. Common indicators include unusual purchase amounts, abnormal geographic locations, and repeated failed attempts.

- **3D Secure Authentication (3DS)**

3D Secure is an additional security protocol implemented by card networks like Visa (Verified by Visa), MasterCard (SecureCode), and others. It prompts customers to authenticate a transaction using a password, OTP, or biometric verification before it is processed. This helps confirm the legitimacy of the transaction and reduces chargebacks and fraudulent claims.

- **Secure Payment Gateways and APIs**

Established payment service providers such as PayPal, Stripe, and Razorpay offer secure APIs that integrate with e-commerce platforms to manage payments. These gateways implement all major security protocols, including encryption, 2FA, tokenization, and compliance checks, ensuring that customer and merchant data remain protected throughout the transaction process.

## V. PROPOSED SYSTEM

The proposed system aims to develop a **blockchain-based secure payment gateway** for e-commerce platforms. This system addresses the security, transparency, and cost-related limitations of traditional centralized payment gateways by leveraging blockchain technology and smart contracts for decentralized, tamper-proof, and real-time transactions. The system uses cryptographic techniques to secure user data and prevent unauthorized access. Each transaction is time-stamped and validated through a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring that all parties have a unified view of the transaction history.

- **Decentralized Payment Processing**

The system eliminates the need for centralized intermediaries by facilitating peer-to-peer transactions through blockchain. Each payment is recorded on a distributed ledger that is accessible to all participating nodes, ensuring transparency and reducing the risk of fraud or manipulation.

- **Use of Smart Contracts**

Smart contracts are deployed to automate and enforce the rules of each transaction. Once predefined conditions are met—such as confirmation of order delivery—the smart contract executes the payment automatically. This minimizes human intervention and improves trust between buyers and sellers.

- **Cryptocurrency and Token Integration**

The system supports cryptocurrency wallets and can handle payments using digital assets such as stablecoins or tokens backed by fiat currency. This allows for fast, borderless, and secure transactions while minimizing currency conversion issues.

## VI. METHODOLOGY

### MODULE DESCRIPTION

#### 1. E-Commerce Web Application

This module represents the front-facing platform where users interact with the system. It is developed using Python, Flask, MySQL, Bootstrap, and hosted on WAMP Server. It consists of essential features of an e-commerce system such as user registration, login, product browsing, cart management, and order placement. Flask handles server-side logic and routing, while MySQL is used to store user and product information. Bootstrap ensures a responsive and user-friendly UI. This module serves as the foundation of the platform, connecting the front end with backend services, including the payment and blockchain modules.

#### 2. Payment Gateway

The Payment Gateway acts as the intermediary between buyers and sellers for initiating and confirming payments. Instead of using traditional centralized third-party gateways, this module integrates with the blockchain to validate transactions through smart contracts. It handles the generation of transaction requests, captures payment details from the user, and securely transfers data to the blockchain layer. This module ensures smooth communication between the e-commerce platform and the blockchain ledger, while maintaining accuracy and reliability of the transaction process.

#### 3. Blockchain Integration

This module is responsible for integrating a private blockchain network built using JSON-based structures. It maintains a decentralized ledger for all transactions, ensuring data immutability and transparency. Each transaction is converted into a block containing transaction details, time stamps, and cryptographic hashes. This block is then added

to the blockchain after validation. This module eliminates the need for third-party verification, thereby improving security, reducing processing time, and ensuring trust in the payment process.

#### 4. System User

This module manages the different roles and functionalities of users in the system:

- **Admin:** Manages the platform, monitors transactions, handles disputes, and oversees the system's integrity.
- **Seller:** Uploads products, manages inventory, views payment statuses, and receives updates via blockchain.
- **Buyer:** Browses products, places orders, initiates payments, and tracks order and payment status.
- Role-based access control ensures that each user type only accesses relevant features and data.

#### 5. Payment Processing

This module handles the core logic for conducting payments. It verifies transaction requests, executes smart contracts, validates transactions using the consensus mechanism, and adds them to the blockchain. It ensures that payment is processed only when both parties (buyer and seller) fulfill the transaction conditions. It includes confirmation messages, transaction receipts, and integration with cryptocurrency or token balances if applicable. The module focuses on providing a seamless and real-time experience to the users.

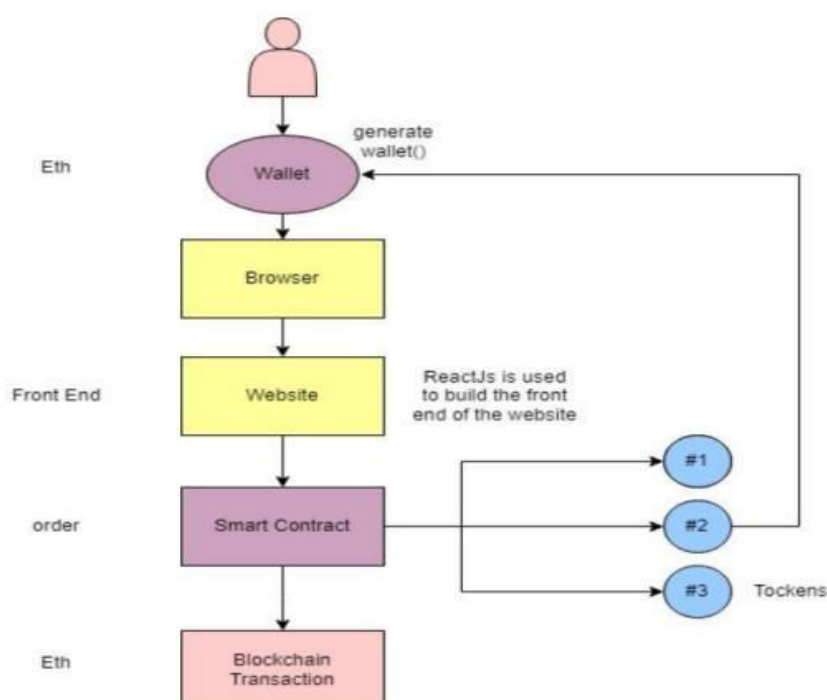
#### 6. Security and Encryption

Security is central to the entire architecture. This module employs encryption techniques, such as SHA-256 hashing, public/private key cryptography, and secure data transmission protocols to ensure data confidentiality and integrity. All sensitive information such as user credentials, wallet data, and transaction records are encrypted before storage or transmission. It also manages authentication mechanisms and access controls to prevent unauthorized access and fraud.

#### 7. Transaction History and Audit

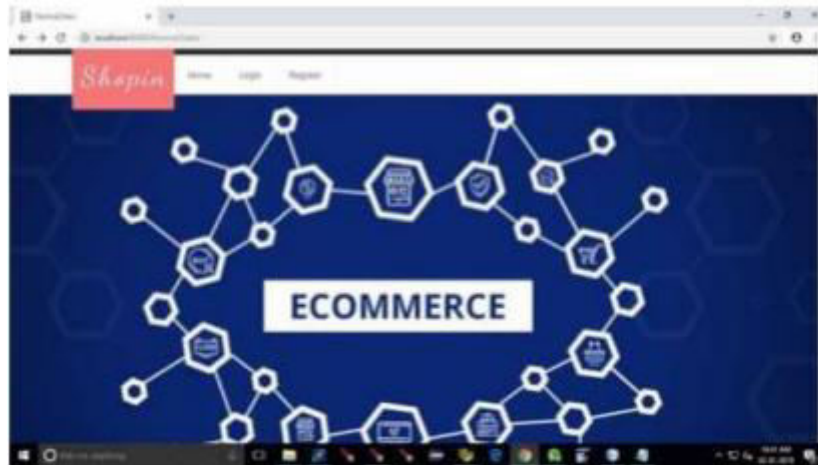
This module logs and displays all transactions made on the platform in a secure, readable format. Every transaction added to the blockchain includes a timestamp, sender/receiver details, amount, and status. Users can access their individual transaction history, while the admin can audit and analyze payment trends, discrepancies, or issues. This module ensures transparency and traceability, which are essential for resolving disputes and maintaining user trust.

### VII. SYSTEM ARCHTECTURE





## VIII. EXPERIMENTAL RESULTS



## IX. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN E-COMMERCE

The benefits of integrating blockchain technology with e-commerce are numerous and include identity verification, loyalty programs, and administration of digital property and inventories. Integrating creativity and prediction with security and transparency allows corporate entities to make the best use of the elements of the blockchain technology that enhances productivity, protects digital assets, and improves the overall customer experience. The coupling of these two technologies will engender revolution and innovation in e-commerce thus creating safer and more efficient and customer-centric processes.



## X. CONCLUSION

In conclusion, this project introduces a blockchain-based secure payment gateway tailored for e-commerce platforms, addressing many of the limitations found in traditional centralized systems. The increasing reliance on digital transactions in the modern world demands greater security, transparency, and efficiency — all of which are achieved through the decentralized nature of blockchain technology. By implementing a private blockchain using JSON and integrating it seamlessly into a Python-Flask-based e-commerce web application, the project ensures that transactions are tamper-proof, transparent, and cryptographically secure. Smart contracts automate the payment process,

reducing dependency on third-party intermediaries and minimizing the risk of human error or manipulation. The use of encryption algorithms and secure authentication further protects user data and payment credentials. Additionally, with modules designed for different system users — including admin, seller, and buyer — the platform offers a full-featured, role-based, scalable architecture. Overall, the proposed system enhances transaction trust, reduces operational costs, and offers a future-proof solution for secure digital commerce.

#### **XI. FUTURE WORK**

1. Country-specific regulatory aspects as well as comparison studies on e-commerce can be done.
2. Scalability Solutions: Future work could focus on developing scalable blockchain solutions that can handle a higher volume of transactions without sacrificing performance. This may involve advancements in consensus algorithms, sharding techniques, or layer-two solutions like state channels or sidechains.
3. Privacy and Confidentiality: Enhancing privacy and confidentiality in blockchain-based e-commerce payments is an important area for future research. Exploring techniques such as zero-knowledge proofs, secure multiparty computation, or privacy-enhancing frameworks can enable confidential transactions without compromising the transparency and auditability aspects of blockchain.

#### **REFERENCES**

1. Fubao He, Yilai Zhang, Tongjun Guo, Yuhua Zha, “Multi-supplier Selection Model Research of Ceramic E-commerce Distribution Platform ” 978-0-7695-5004-6/13 \$26.00 © 2013 IEEE DOI 10.1109/ICCIS.2013.171.
2. Li Lin, “E-Commerce Data Analysis Based on Big Data and Artificial Intelligence ” 978-1-7281-3977-7/19/\$31.00 ©2019 IEEE DOI 10.1109/ICCNEA.2019.00034.
3. Sarah S. Alrumiah and Mohammed Hadwan, “Implementing Big Data Analytics in E-Commerce: Vendor and Customer View ” VOLUME 9, 2021.
4. Tong Liu, “Research on the Design of E-commerce Data Analysis Platform ” 978-1-6654-3873-5/21/\$31.00 ©2021 IEEE DOI 10.1109/ECIT52743.2021.00034.
5. Qiao Tan, “Research on E-Commerce Security and Data Analysis Platform in the Era of Big Data ” 978-1-7281-9638-1/201/\$31.00 ©2020 IEEE DOI 10.1109/MLBDBI51377.2020.00087.
6. Adhitya Bhawiyuga, M. Ali Fauzi, Eko Sakti Pramukantoro, Widhi Yahya, “Design of E-Commerce Chat Robot for Automatically Answering Customer Question ” 978-1-5386-2182-0/17/\$31.00 c 2017 IEEE.
7. Pon Sangeetha. J, Ramya. S. S, Christal. Antony. V, Mythili. K, “Secured payment gateway for authorizing Ecommerce websites and transactions using Machine Learning Algorithm ” 978-1-7281-4514-3/201/\$31.00 ©2020 IEEE.
8. Safwan Hossain, Akiba Mehzaheen Mon, Rakib Hasan, “Implementation of A Multivendor E-commerce Website ”.
9. E. Turban, J. Outland, D. King, K. J. Lee, P. T, Electronic Commerce 2018: A Managerial and Social Networks Perspective : Springer 2017.
10. Q. Yu, The Theory and Practice of Combining Social Networking and E-commerce, Central China Normal University, April. 2015.

#### **BOOK REFERENCES**

1. Python – Mark Lutz, “Learning Python,” 5th Edition, O’Reilly Media, 2013.
2. MySQL – Paul DuBois, “MySQL Cookbook,” 3rd Edition, O’Reilly Media, 2014.
3. HTML – Jon Duckett, “HTML and CSS: Design and Build Websites,” Wiley, 2011.
4. CSS – Eric A. Meyer, “CSS: The Definitive Guide,” 4th Edition, O’Reilly Media, 2017.
5. JavaScript – David Flanagan, “JavaScript: The Definitive Guide,” 6th Edition, O’Reilly Media, 2011.
6. JSON – Lindsay Bassett, “Introduction to JavaScript Object Notation,” O’Reilly Media, 2015.





INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details