RESEARCH PAPER

Securing E-Commerce Payments using Decentralized Crypto Escrow

S. Praveena[1], T. Arasulingam[2], M. Dineshkumar[3], P. Puvirajan[4], Jean Deiva[5], P. Rajasozhan[6], H. Vinayak rakecha[7]

[1]Assistant Professor, [234567] UG Scholars,

Department of Artificial Intelligence and Machine Learning,
Manakula Vinayagar Institute of Technology, Puducherry

ABSTRACT

The rapid expansion of digital commerce has brought forward new challenges in payment security and transactional trust. Buyers and sellers engaging in online platforms face persistent threats such as payment fraud, unauthorized fund diversions, delayed settlements, and an overreliance on centralized financial intermediaries. Traditional mechanisms, which route payments through banks and payment gateway providers, often introduce additional costs while creating points of vulnerability that undermine consumer confidence. This paper proposes a blockchain-driven decentralized crypto escrow payment framework designed to address these shortcomings in a fundamental way. Rather than routing buyer payments directly to merchant accounts, the system temporarily secures those funds within a smart contract-governed escrow until all agreed-upon transaction conditions have been satisfied — including verified order fulfilment and successful product delivery. In the event of a dispute or transaction failure, the system enforces pre-coded refund protocols without requiring manual intervention. The proposed framework is expected to strengthen the relationship between buyers and sellers, meaningfully raise the bar for payment security, and deliver a transparent, auditable transaction environment through the principles of decentralized finance.

Keywords: Decentralized Crypto Escrow, Blockchain Technology, Smart Contracts, Cryptocurrency Transactions, Transaction Verification, Block chain-Based Escrow, Secure Online Transactions.

How to cite this article: Praveena S, Arasulingam T, Dineshkumar M, Puvirajan P, Deiva J, Rajasozhan P, Vinayak rakecha H. Securing E-Commerce Payments using Decentralized Crypto Escrow. Int J Drug Deliv Technol. 2026;16(55s): 51-57. DOI: 10.25258/ijddt.16.55s.5

Source of support: Nil.

Conflict of interest: None.

INTRODUCTION

Digital retail has woven itself deeply into the everyday lives of people across the globe, reshaping how individuals purchase goods, access services, and conduct financial exchanges. The emergence of internet-enabled commerce platforms has removed geographic barriers that once limited buying and selling, allowing consumers to engage with merchants from virtually any location at any time. As broadband penetration has widened and smartphone usage has surged, the volume of financial transactions flowing through e-commerce channels has grown exponentially. Yet this growth has not come without complications. Alongside the convenience of online shopping, a range of security and trust-related challenges has surfaced. Buyers worry about fraudulent sellers who disappear after receiving payment, while sellers contend with the risk of dishonest customers disputing legitimate transactions. These mutual anxieties create friction within the online marketplace and erode the confidence needed for digital commerce to function smoothly.

Smart contracts, self-executing programs deployed on blockchain networks, have emerged as a promising instrument for eliminating intermediary dependency in transaction workflows. By encoding transaction conditions directly into immutable code, smart contracts can automatically release or withhold payments based on whether agreed criteria have been fulfilled. This capacity for autonomous execution removes the need for third-party adjudication and reduces the window for human error or manipulation.

Blockchain technology, with its distributed ledger architecture, adds another layer of resilience by

ensuring that no single entity controls or can tamper with the transaction record. Data is replicated across many nodes simultaneously, making unauthorized modification computationally prohibitive. When applied to e-commerce payment flows, this infrastructure provides a foundation for building systems that are both highly secure and inherently transparent. The present work builds on these foundations to propose a practical crypto escrow mechanism suited for real-world digital commerce applications.

IMPORTANCE

The significance of a decentralized crypto escrow framework extends beyond technical innovation — it addresses a genuine gap in how online transactions are governed today. For buyers, the assurance that their funds remain protected within a neutral contract until delivery is confirmed substantially reduces the psychological barrier associated with online purchases. For sellers, the system provides clarity around payment legitimacy and a defined structure for handling disputes, reducing the risk of fraudulent chargebacks.

Eliminating the role of centralized intermediaries also carries economic implications. Traditional payment processors charge transaction fees that, while individually small, accumulate into significant costs for merchants operating at scale. By routing funds through a smart contract on a blockchain network rather than through a financial institution, the system reduces per-transaction costs and removes potential bottlenecks caused by institutional processing delays. The result is a payment environment that is faster, cheaper, and more equitable for all parties involved.

EXISTING METHODS

Contemporary e-commerce ecosystems rely heavily on centralized payment infrastructure. When a customer initiates a purchase, their payment typically flows through a payment gateway before being routed to the merchant's bank account. Entities such as commercial banks, card networks, and third-party payment processors serve as intermediaries, validating the transaction and guaranteeing the transfer of funds. While these mechanisms are mature and widely adopted, they carry notable drawbacks.

The most immediate concern is the cost overhead associated with intermediary involvement. Each ntity in the payment chain levies its own fees, which ultimately reduce merchant margins or get passed on to consumers. More critically, centralized systems create single points of failure — either in terms of security vulnerabilities or institutional trust. A compromised payment gateway or a bank that freezes accounts mid-transaction can halt commerce entirely.

Transparency is another area where current systems fall short. Buyers often have limited visibility into where their funds are at any given stage of the transaction, and dispute resolution processes can be opaque and slow. Fraudulent transactions, fictitious product listings, and delayed refunds are recurring complaints among online shoppers. These persistent issues indicate that the existing payment infrastructure, despite its widespread use, is not sufficiently equipped to handle the trust demands of modern digital commerce.

MODEL DESCRIPTION

To better understand the value of the proposed system, it is useful to contrast its design with that of conventional payment flows. In the traditional model, a customer completes a checkout process on an e-commerce website and submits payment through an integrated gateway. The funds are transferred to the seller's account immediately upon transaction approval, regardless of whether the goods have actually been shipped or received. The buyer's only recourse in the event of non-delivery is to file a dispute with the payment provider — a process that can take weeks and does not always result in restitution.

The proposed decentralized crypto escrow model inverts this dynamic. When a buyer initiates a purchase, their payment is directed into a smart contract that holds the funds in escrow rather than forwarding them to the seller. The contract is programmed with specific release conditions — most critically, confirmation of successful delivery. Only when the system receives verified confirmation that the transaction conditions have been met does the contract automatically release the funds to the seller. This design ensures that neither party bears disproportionate risk during the transaction lifecycle.

Should the transaction fail — whether due to non-delivery, a dispute, or a breach of the agreed terms — the system executes a pre-defined refund protocol, returning the escrowed funds to the buyer without requiring manual adjudication. This built-in dispute-handling mechanism represents a significant improvement over the ad hoc complaint processes that characterize most current e-commerce platforms.

SYSTEM MODEL

Implementation Approach and Validation

Data Gathering

The decentralized cryptocurrency escrow system accumulates transactional data as users interact with the platform throughout the purchasing process. The information captured includes buyer and seller identities, transaction request parameters, payment status indicators, order confirmation events, and timestamped records of each transaction stage. This data serves as the input for the smart contract evaluation and audit processes.

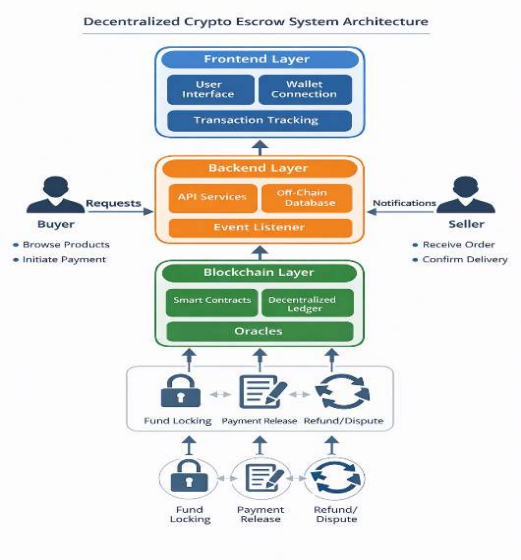
Data Preprocessing

Before any transaction is processed through the smart contract layer, the collected data undergoes a preprocessing stage to ensure its consistency and integrity. This step involves identifying and discarding redundant, erroneous, or incomplete entries, as well as formatting the cleaned data into a structure compatible with the smart contract execution environment. Consistent data quality is essential to ensuring that contract conditions are evaluated correctly and that payment decisions are based on accurate information.

Feature Engineering

Identifying the transaction attributes most relevant to secure payment processing is central to the feature engineering component of the system. The following transaction features are defined and tracked within the escrow workflow:

- Transaction Verification Feature: validates the identity and details of both the buyer and the seller before any funds are committed.
- Payment Status Feature: tracks the progression of the payment through each stage of the transaction lifecycle.
- Escrow Tracking Feature: monitors the locked funds within the smart contract and records their status.
- Transaction History Feature: maintains a permanent log of all prior payment activities associated with a given account.



- Delivery Confirmation Feature: verifies whether the conditions for transaction completion — specifically product delivery — have been satisfied.

Together, these features provide the system with the data it needs to execute escrow operations reliably and to support detailed post-transaction review.

PROPOSED SYSTEM

The core proposition of this work is a decentralized crypto escrow mechanism that redefines how payment security is enforced in e-commerce environments. Rather than relying on institutional trust, the system places trust in transparent, immutable code. Every transaction passing through the platform is subject to the same contractual conditions, with payment release governed entirely by whether those conditions have been met — not by the discretion of any single party.

Transaction initiation begins when a customer places an order on the platform and commits payment through a blockchain interface. The transferred cryptocurrency is locked within the escrow smart contract, where it remains until the fulfillment criteria are verified. These criteria principally include order acknowledgment by the seller and independent confirmation that the ordered items have been delivered to the buyer.

In cases where the transaction does not progress as expected — for instance, if the seller fails to dispatch the goods within an agreed timeframe or if the buyer reports a delivery failure — the contract's refund logic is triggered automatically. This process occurs without requiring the buyer to formally escalate a complaint, reducing friction and ensuring timely resolution. By

automating both payment release and refund handling, the proposed system reduces the exposure of both parties to bad-faith behaviour and systemic failure.

WORKING

The operational sequence of the decentralized crypto escrow system follows a structured series of stages, each designed to uphold transactional fairness and minimize the opportunity for exploitation.

Stage One: Transaction Initiation

The process begins when a buyer selects a product on the e-commerce platform and proceeds to checkout. At this stage, the buyer's account details, the seller's identity, and the transaction amount are captured and passed to the smart contract layer for validation.

Stage Two: Payment Locking

Unlike conventional checkout flows where payment is immediately transferred to the seller, the proposed system diverts the buyer's payment into the escrow smart contract. The funds remain locked at this stage, inaccessible to either party, until the relevant transaction conditions are fulfilled. This holding mechanism is enforced entirely by the blockchain protocol, eliminating the possibility of premature or unauthorized fund release.

Stage Three: Transaction Verification

During this phase, the smart contract validates all relevant transaction parameters. This includes confirming payment receipt, verifying the authenticity of the order, and cross-checking delivery status data as it becomes available. Any inconsistencies detected at this stage can trigger a hold or initiate the dispute resolution process.

Stage Four: Delivery Confirmation

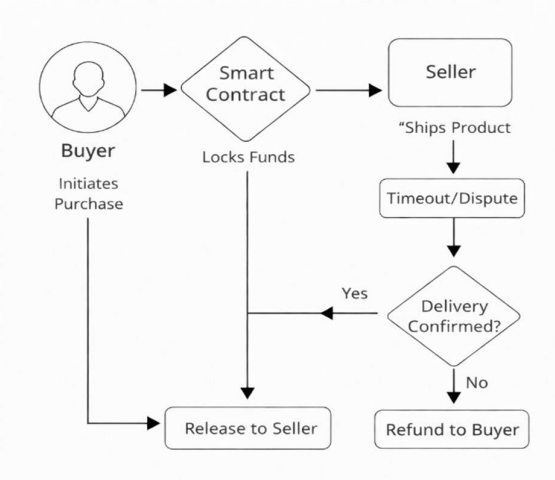
Upon the buyer confirming that the ordered product has been received in satisfactory condition, this confirmation is logged on the blockchain. This event serves as the trigger for the final phase of the payment lifecycle.

Stage Five: Payment Release and Refund Processing

Where delivery is confirmed and all contract conditions are met, the smart contract automatically releases the escrowed funds to the seller. In the event of a dispute or unmet condition, the refund protocol is executed according to the rules encoded in the contract, returning funds to the buyer without delay.

NETWORK ARCHITECTURE

The network architecture underpinning the decentralized crypto escrow system is structured in layers, each serving a distinct function within the broader transaction workflow. This layered design ensures that the system is modular, scalable, and capable of handling transactions at the volume demanded by active e-commerce environments.



User Layer

At the highest level of the architecture sits the user layer, which encompasses both buyers and sellers interacting with the platform. Buyers use this layer to browse product listings, initiate purchases, and confirm delivery. Sellers manage their inventory, process orders, and track payment status through the same layer. The user layer provides the front-end interfaces through which all human interactions with the system take place.

Application Layer

Beneath the user interface lies the application layer, which handles the communication logic between user actions and the underlying blockchain network. This layer is responsible for processing transaction requests, storing order information in a structured format, and coordinating with the smart contract layer to initiate escrow operations. It acts as the intermediary between what users see and what the blockchain executes.

Smart Contract Layer

The smart contract layer is the core operational engine of the system. Contracts deployed at this layer hold buyer payments in escrow, monitor transaction conditions in real time, and autonomously execute payment releases or refunds based on the outcomes of

those conditions. All logic governing fund movement resides at this layer, written in code that is transparent and verifiable by any participant on the network.

Blockchain Network Layer

The blockchain layer provides the distributed ledger on which all transaction records are permanently stored. Each transaction is validated by network nodes through a consensus mechanism before being written to the chain, ensuring that no single entity can alter or delete historical records. This immutability is the foundation of the system's audit capability and its resistance to fraud.

Database and Monitoring Layer

Supporting the blockchain layer is a database and monitoring component that maintains structured records of transaction histories, payment statuses, and user account information. This layer enables platform operators and users to query past transactions, track pending payments, and access audit trails as needed.

Security and Validation Layer

A dedicated security and validation layer underpins the entire architecture, providing cryptographic verification of transaction participants and ensuring that only authorized operations are permitted at each stage of the escrow workflow. This layer also implements fraud detection logic to flag anomalous transaction patterns before they can cause harm.

NOVEL ALGORITHM

The algorithmic approach underlying the proposed crypto escrow system combines conventional transaction logic with blockchain-native execution to create a reliable, automated payment governance framework. The algorithm is parameterized by the transaction conditions agreed upon by buyer and seller at the time of order placement, and it operates through the following sequential logic.

In the first step, the buyer identifies a suitable product on the platform and initiates the transaction by submitting their payment credentials along with details of the order, including product specifications, agreed price, and expected delivery parameters. The system validates these inputs before moving to the next stage.

In the second step, a smart contract instance is deployed on the blockchain to govern the specific transaction. The buyer's payment is transferred into the contract's escrow holding structure rather than to the seller directly. The contract begins monitoring for the fulfilment conditions that would authorize payment release.

The third step involves continuous monitoring and verification. The contract evaluates incoming data — including payment confirmation signals, order status updates, and delivery reports — against the predefined conditions. This evaluation occurs in real time, with the contract autonomously advancing or halting the transaction based on what the data reveals.

In the final step, a resolved transaction results in automatic fund transfer to the seller. Where conditions are unmet or a dispute has been raised, the contract executes the applicable refund instruction and returns the escrowed funds to the buyer. This four-step execution model provides a clean, auditable record of every decision taken throughout the transaction lifecycle, reinforcing accountability on both sides of the exchange.

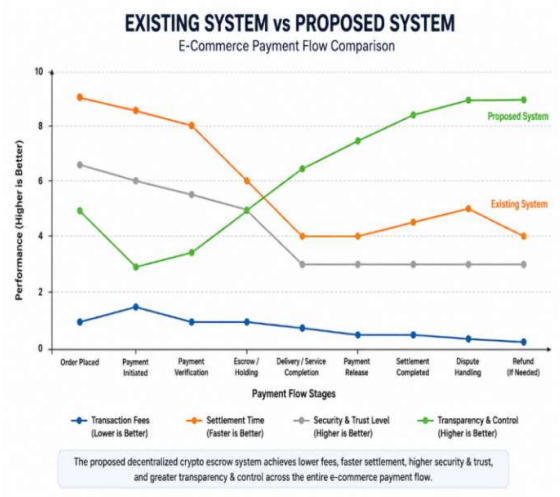
SUMMARY

Present-day e-commerce payment infrastructure is largely built around centralized models in which banks, payment gateways, and third-party processors hold authority over fund flows. While these systems are operationally mature, they are burdened by structural limitations including security gaps, slow dispute resolution, high transaction costs, and fragile trust dynamics between buyers and sellers. These challenges are amplified as transaction volumes grow and as bad actors become increasingly sophisticated in exploiting vulnerabilities within centralized systems.

A particularly acute weakness of current approaches is the practice of releasing buyer funds before delivery is confirmed. This asymmetry places undue financial risk on buyers and creates opportunities for fraudulent sellers to exploit the gap between payment and delivery. The proposed decentralized crypto escrow system eliminates this asymmetry by ensuring that funds remain in neutral custody until both parties have met their obligations.

The system's use of smart contracts provides a mechanism for enforcing transaction rules consistently and transparently, without relying on institutional oversight. The blockchain record ensures that all transaction events are permanently logged and accessible for verification, providing a level of accountability that centralized systems struggle to match. Taken together, these features position the proposed framework as a meaningful advance in the

design of secure, fair, and efficient e-commerce payment systems.



CONCLUSION

This paper has introduced a decentralized crypto escrow payment system as a viable solution to the trust and security deficiencies that continue to limit the potential of online commerce. By securing buyer funds within a smart contract until delivery conditions are verified, the system removes the structural vulnerability that allows fraudulent transactions to succeed under conventional payment flows. Payment release and refund decisions are automated through immutable blockchain code, reducing reliance on human adjudication and ensuring that outcomes are governed by agreed rules rather than institutional discretion.

The experiment of routing payments through smart contracts demonstrates that it is technically feasible to build a reliable, transparent transaction system without involving centralized intermediaries. Buyers gain meaningful protection against fraud and non-delivery, while sellers benefit from a structured and tamper-proof payment confirmation mechanism. The blockchain foundation ensures that all records are preserved in an auditable form, which supports accountability across the full transaction lifecycle.

The framework also contributes to a more equitable transaction environment by ensuring that both buyers and sellers operate under the same contractual rules. Dispute handling is encoded at the contract level, meaning outcomes are predictable and consistent rather than subject to the vagaries of third-party review. This consistency is likely to improve confidence in e-commerce as a medium for financial exchange, particularly as blockchain adoption becomes more widespread.

FUTURE WORKS

While the proposed system provides a strong foundation for secure decentralized e-commerce payments, several avenues for further development have been identified. One priority area is the refinement of dispute resolution mechanisms to handle more nuanced transaction scenarios — for example, partial deliveries, quality disputes, and multi-stage fulfilment agreements. Incorporating arbitration logic that can accommodate a broader range of real-world transaction patterns would substantially increase the practical utility of the platform.

Another prospective enhancement involves extending the system's compatibility to operate across multiple blockchain networks and to integrate with cloud-based deployment infrastructure. This would improve scalability and allow the escrow framework to be accessed by users operating in different cryptocurrency ecosystems. Cross-chain interoperability is a recognized challenge in the blockchain space, and progress in this area would expand the addressable market for the proposed system considerably.

The integration of advanced analytics and intelligent behavioural monitoring represents a further area of potential. Machine learning models trained on transaction data could detect unusual patterns that suggest fraudulent intent before a transaction completes, adding a proactive layer of defence to the system's reactive refund protocols. Such capabilities would improve the overall resilience of the platform against increasingly sophisticated forms of payment fraud.

Finally, future development efforts should prioritize the creation of accessible mobile interfaces and role-specific dashboards for administrators, merchants, and consumers. Improved front-end tooling would lower the barrier to entry for non-technical users and ensure that the security benefits of the system can be realized by a wide and diverse user base. These combined improvements would move the platform closer to a production-ready solution capable of competing with established commercial payment systems.

REFERENCES

[1] Asgaonkar, A., & Bhaskar Krishnamachari (2019). Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator. International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–9.

[2] Kamal Kishor Singh (2022). Application of Blockchain Smart Contracts in E-Commerce and Government. Research Study on Smart Contracts and E-Commerce Applications.

[3] Khan, S. N., et al. (2021). Blockchain Smart Contracts: Applications, Challenges and Future Trends. Journal of Systems Architecture.

[4] Tolamise Olasehinde (2025). Smart Contracts in E-Commerce: Automating Transactions and Reducing Fraud with Blockchain. International Research Study on E-Commerce Automation.

[5] Werner, S. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Financial Technology Review.

[6] Alharby, M., & van Moorsel, A. (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study. Journal of Computer Science Research.

[7] Schwartzbach, N. I. (2020). An Incentive-Compatible Smart Contract for Decentralized Commerce. Blockchain Commerce Research Study.

[8] Staples, M., et al. (2017). Risks and Opportunities for Systems Using Blockchain and Smart Contracts. Technical Research Report.

[9] Singh, K. K. (2022). Blockchain Applications in E-Commerce Business Models. International Journal of Blockchain Technology.

[10] Bassan, F. (2024). From Smart Legal Contracts to Contracts on Blockchain. International Journal of Law and Digital Technology.

[11] Hariyani, D. (2025). A Literature Review on Transformative Impacts of Blockchain Technology. Engineering and Technology Review.

[12] Ali, A. (2022). Decentralized Escrow Protocol for Secure Payment Systems Using Smart Contracts. Blockchain Security Research Study.

[13] Guntara, R. G. (2023). Blockchain Implementation in E-Commerce to Improve Transaction Security. Journal of Research in Engineering and Technology.

[14] Brent, L., et al. (2018). Vandal: A Scalable Security Analysis Framework for Smart Contracts. Security Systems Research.

[15] Chantal Bomprezzi (2021). Implications of Blockchain-Based Smart Contracts on Contract Law. Research Thesis on Blockchain Legal Frameworks.

[16] Rathakrishnan, A., et al. (2024). A Trustable Real Estate Transaction Based on Public Blockchain: A Smart Contract-Driven Framework.

[17] Building a Smart Contract Based Escrow Platform. International Journal of Creative Research Thoughts, Vol. 11, Issue 6, 2023.

[18] Smart Contract Based E-Commerce Payment Gateway. International Journal of Scientific Development and Research, Vol. 8, Issue 5, 2023.

[19] Use of Smart Contracts as Digital Agreements in Blockchain E-Commerce Systems. International Journal of Engineering Science and Technology, 2025.

[20] Digital Escrow and Conditional Payment Logic Using Blockchain for Cross-Border Trade. International Journal of Web and Open Systems, 2025.