



Blockchain - Driven Trust Management for Secure and Transparent Online Commerce

Rohini V¹, Dr.V.Priyalakshmi²

¹Assistant Professor MBA S A College Of Arts And Science,
Poonamallee, Avadi Rd, Viraraghavapuram,
Thiruverkadu, Chennai, Senneerkuppam, Tamil Nadu 600077
Rohiniv@Sacas.Ac.In

²Assistant Professor Department Of Bsc Cs With Cognitive Systems Sdnb Vaishnav College For Women , Chrompet
State: Tamilnadu
Priyalakshmi.V@Sdnbvc.Edu.In

Abstract- Despite the growing success of online commerce, problems such as fraud and lack of transparent reputation schemes are still present and represent single points of failure in the current intermediary-based models. In this regard, the following paper suggests the development of blockchain-based trust management system which would provide for trustworthy verification of participants' identities, smart-contract based escrow, and reputation scoring on-chain. The suggested methodology implies the use of W3C-compliant Decentralized Identifiers, two-blockchain system, and automated dispute resolution mechanism. Further comparative evaluation of the suggested system in terms of transparency, fraud prevention and implications for international trade is conducted. The paper concludes that the suggested trust management infrastructure represents a structurally robust solution to centralized reputation models.

Key Word: Blockchain, Trust Management, E-Commerce, Smart Contracts, Decentralized Identity, Reputation Systems, Verifiable Credentials

I. INTRODUCTION

E-commerce has revolutionized the business environment, facilitating the execution of transactions irrespective of geographical locations with no physical presence or pre-existing relationships between the parties involved. This separation from the need for physical interaction, however, has created a significant challenge – the need for the establishment of trust not through physical interactions or jurisdiction but via technological and institutional means. The predominant way in which trust has been created is via centralized intermediary platforms including marketplaces, payment services, and escrow facilities, whose scale and information aggregation allows them to create security promises. Examples include amazon, ebay, alibaba, and similar companies, whose value propositions are premised upon their ability to create safe transactional environments [2][6].

But centralized trust systems have built-in vulnerabilities that can be remedied through blockchain. Firstly, centralized systems have inherent flaws since they are single points of failures; breaches of security, fraud by insiders, or interruptions during operations can make the trust system ineffective for all transactions. Secondly, the business model of such centralized systems leads to the creation of flawed incentives; the intermediary's need for profit maximization

is not always aligned with the needs of consumers and sellers, and this can be seen through algorithmic opacity, data exploitation, and fees from both parties of transactions. Thirdly, reputation information is kept only on each individual platform without being portable to allow sellers to use their reputation elsewhere and help buyers in aggregate reputational judgments. Finally, there could be manipulations of reputation information when economic and regulatory pressures arise [2][5][6][9].

Blockchain technology provides a completely different approach for managing trust. Due to distributed transactions' validation and immutable ledgers, blockchain provides the possibility of eliminating the need for trust in central authorities while ensuring the cryptographic guarantees of data integrity [2][10]. The implementation of smart contracts allows automated execution of conditions without any further action of humans or involvement of third parties [1][3][7]. Also, decentralized identifiers and verifiable credentials provide opportunities for proving the participant's attributes and authorizations without disclosing unnecessary data about their personal information [4][8].

Many studies have been devoted to the integration of these tools into trust management architectures. Some studies consider blockchain-based reputation systems, which guarantee anonymity of reviewers [5][9], two-blockchain architecture, where the identity is separated from transaction processing [9], and hybrid architectures that combine



blockchain with iot devices to implement supply chain verification [1]. However, there are many open questions regarding the synthesis of all these elements into one complete trust architecture, which covers the entire process of commercial communication – from the registration of participants to dispute settlement. Moreover, there is a lack of comparative evaluation of performance of blockchain-based trust management compared to other centralized approaches [1][5][6].

There are three main points presented by this paper. First, a framework for building a blockchain-based trust management system for e-commerce is suggested which combines decentralization of identification process, smart contract escrow mechanism, and reputation scoring. Second, the features of the framework Are considered in connection with its operation in comparison with centralized systems of trust. Third, the problems to be solved when implementing such a system are highlighted.

II. LITERATURE SURVEY

There are many streams of research regarding the application of blockchain technology for trust management in electronic commerce. The early research laid down the basic theory of blockchain reputation by proving that it was possible to keep tamper-proof records of feedback without any central authority [2][9]. Zhou et al. Suggested a reputation system for blockchain based on feedback ratings that can be verified by anyone but cannot be changed afterward. The basic structure solved the basic problem in the centralized reputation mechanism that the platform could change or hide any feedback, but it brought some other problems that have been discussed later [9].

Privacy in blockchain reputation systems has been an especially vibrant research field. The authors of Visorfair Presented a technique using fair signature exchange and adaptor signatures to ensure atomic transactions in which reviewers would rate the service provider only after completing a transaction, without revealing the identity of the reviewer [5]. This approach is designed to address the problem of service providers manipulating their review token to prevent getting any negative reviews, which is possible through the centralized architecture of platforms but not within a blockchain structure [5]. Likewise, the two-blockchain framework for hyperledger indy and fabric, developed by researchers from salem, showed how verifiable credentials can secure the identity of vendors while ensuring the integrity of the reputation system [9].

The use of smart contracts in e-commerce trust management models has led to the development of automatic enforcement processes that reduce the need for manual dispute resolution procedures [1][3]. The blockchain enabled trust management system for cross-border e-commerce utilizes smart contracts

that make automatic payments upon Fulfillment Of delivery period and quality requirements by means of iot sensors [1]. Such a model solves the problem of the payment versus delivery race condition prevalent in cross-border commerce due to the fact that the buyers and sellers are located in different legal jurisdictions [1]. Crowdfunding applications based on ethereum smart contracts serve as examples of such systems [3][7].

It has become apparent that decentralized identity management is an integral part of any trust architecture built on blockchain technology. The decentralized identifier standard and verifiable credentials model developed by the w3c ensure interoperability in the representation of identity characteristics that may be verified cryptographically while hiding extra information [4][8]. Work done in the area of agent authorization frameworks takes this idea a step further, offering bounded delegation credentials that define the scope, spending limits, and time intervals [4]. This technology has special importance in relation to the new agentic commerce protocols, where ai shopping assistants conduct transactions on behalf of humans [4].

Studies on consumer behaviour offer valuable insights into perceived benefits of blockchain regarding trust. For instance, research using survey data about the features of blockchain in e-commerce has found that transparency and security are the key factors that affect the formation of trust, whereas cost reduction affects the value perception only [6]. The study also revealed that retail familiarity is a moderating factor in the Trust creation mechanism of blockchain, which means that well-established companies benefit less from the technology because of the guarantee of transparency it offers compared to unfamiliar merchants [6].

Nevertheless, despite such a rich literature, there still are gaps in the understanding of the topic. First of all, the existing frameworks try to solve problems associated with single components, such as reputation, identity, or payments; however, they do not propose any solutions in terms of comprehensive trust management throughout the whole transaction process [1][5][8][9]. Secondly, the evaluation of the approach in terms of comparative analysis with centralized counterparts is mostly qualitative. There is little systematic discussion of the trade-offs related to implementation of the technology [1][2][6][10].

III. PROPOSED METHODOLOGY

1. Framework Overview

The proposed bdtm system functions as a layer-2 system that could be plugged into existing e-commerce systems or act as a marketplace protocol system by itself. The architecture is composed of four distinct layers, namely, identity and onboarding, transactions and escrow, reputation and scoring,



and finally dispute resolution. The high-level system architecture is illustrated in figure 1.

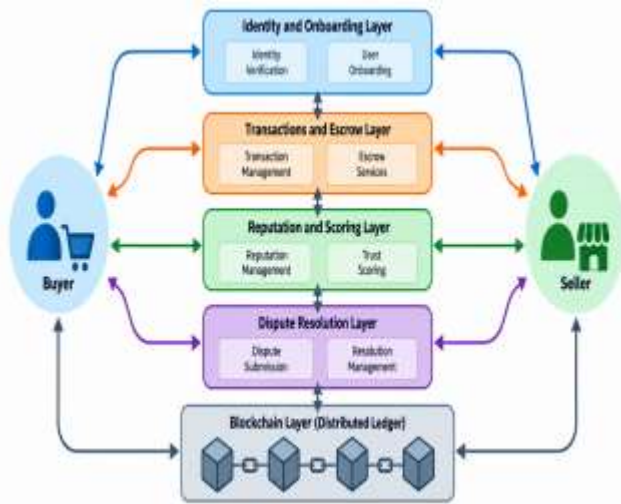


Figure 1: BDTM System Architecture

The approach used by the framework relies on a two-blockchain structure akin to what was tested in previous research works: a permissioned blockchain for identity using hyperledger indy, which is meant to manage decentralized identities and verifiable credentials; and a transactions blockchain using hyperledger fabric, which is tasked with facilitating business transactions and storing reputations.

2. Participant Onboarding and Identity Management

All participants—both buyers and sellers, as well as logistic services—undergo the onboarding process in two stages. The first stage creates a decentralized identifier (did) through the identity chain, thus creating a cryptographic identity without revealing any information about legal identities to counterparts. In the second stage, the business attributes are checked, where sellers present the credentials for business registration, tax identification, and product authorization; buyers may provide reputation anchors from existing platforms through zero-knowledge proofs verifying the account history but not the account identity.

Onboarding gives every participant a starting trust score based on verified attributes and imported reputation data, if any. This trust score will serve as a bayesian prior to be modified through the results of transactions. Figure 2 demonstrates the process of onboarding and credential verification.

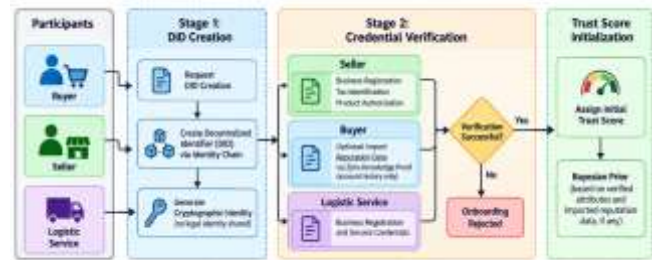


Figure 2: Participant Onboarding Flow

3. Smart Contract Escrow and Automated Settlement

Business-to-business transactions follow smart contracts that enable escrowing of payment from buyer to seller after order confirmation and releasing of payment based on predefined criteria. Criteria can include the confirmation of delivery, confirmation of product conditions while it is being transported using iot sensors, and confirmation of receipt from the buyer within a certain period of time. Escrowing is done using the business transaction chain and uses credentials but does not disclose any personal information.

Smart contract provides for a tiered payment model – part of the payment is given to the seller based on the confirmation of shipment and the rest when there is confirmation of delivery. Such an approach takes into account the requirements of both parties – seller's need for cash flow and buyer's security requirements. It solves one of the weaknesses of the full-escrow approach which imposes too much burden on sellers regarding working capital.

4. On-Chain Reputation Scoring

The reputation scores themselves are stored on-chain as non-transferable scores that represent the accumulation of transaction results, counterparty ratings, and dispute resolution results. The reputation score calculation relies on a weighted exponential decay model that places more emphasis on recent transactions but still takes into account previous transaction history. Reputation scores are tied to the did of the user rather than to any account on a specific platform, making them portable across different platforms.

Several features make the reputation scoring system less susceptible to manipulation. Sybil attack prevention is provided due to the cost associated with identity verification during the onboarding process. Feedback manipulation is prevented since only parties involved in completed transactions can provide ratings and they must prove it cryptographically. Collusion between users for rating manipulation is prevented with the help of graph analysis of transaction and ratings.



5. Decentralized Dispute Resolution

If there are disagreements that cannot be solved using automated contract execution, the disputes will get escalated to the decentralized arbitration pool. Here, arbitrators are chosen among participants who have high reputation scores and are part of the Arbitrator's Pool, where they have locked their collateral and have agreed to lose it in case of incorrect decisions. In the arbitration process, each party submits evidence and a decision is made after reviewing by a randomly chosen arbitrators group using majority voting, while appeals can also be made in the case of high-value disputes.

The results of the arbitration process are recorded on-chain and influence the reputation of all parties participating in the process. Arbitrators that had their decision overturned during the appeals process will get penalized in terms of reputation score and lose their collateral.

IV. ANALYSIS AND DISCUSSION

1. Transparency and Auditability

The bdtm system offers more transparency regarding its structure compared to centralized trust systems. The transactions' details, reputation changes, and decisions in case of disputes can be viewed through an immutable ledger to which only authorized individuals have access. In contrast to centralized systems, where algorithms and data processing procedures are unknown to the user, the bdtm system is more transparent. Figure 3 illustrates transparency differences between trust models.

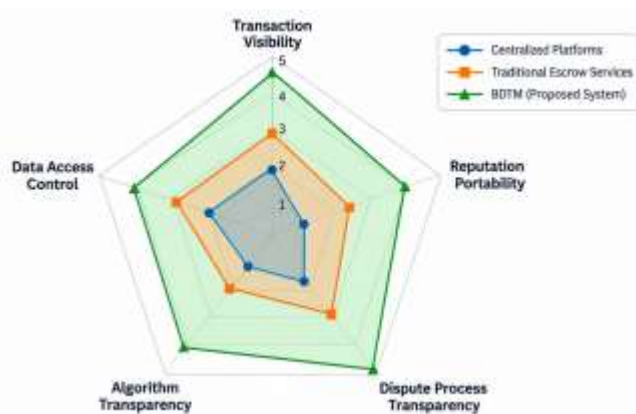


Figure 3: Transparency Comparison Across Trust Models

What follows from this transparency is the fact that fraud detection shifts from being an inherent feature of the platform into being a function performed across the network as a whole. Any user can Analyze Transaction history and detect

unusual behavior. Studies of blockchain fraud detection systems have shown that this immutability allows for backward analysis which could not be done with centralized systems due to data deletion.

2. Fraud Resistance and Security Properties

The security of the platform is provided by the following features. The absence of a single point of failure is ensured by the distributed ledger, which means that breaching trust is not possible without simultaneously breaching a majority of validating nodes instead of a single database. Escrow of smart contract eliminates counterparty risk associated with the payment-versus-delivery problem, as no participant is able to unilaterally change the terms of the contract or withhold funds in violation of the terms.

Resistance to reputation manipulation is provided by the necessity of leaving transaction-linked feedback and the cost of the identity establishment. Modeling Of the economic feasibility of the sybil attack shows that the combination of costs and stakes needed to participate in the dispute resolution process provides reasonable deterrence for massive manipulation, while some skilled attackers with considerable resources may pose a threat in niche markets.

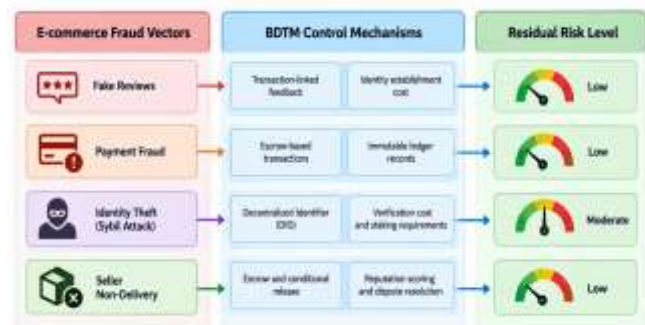


Figure 4: Fraud Vector Resistance Mapping

The cross-border transaction can especially be helped by the qualities that have been described. In traditional cross-border business, there is more than one intermediary involved, namely payment processors, currency exchange services, customs brokers, and logistics companies, each of which adds an extra cost burden and risk to the process.

3. Comparative Analysis

Table i provides a comparative analysis between the bdtm approach and three different trust approaches namely centralized marketplace platforms (E.G. Amazon, ebay), escrow, and permissionless blockchain marketplaces.



Table 1: Comparative Analysis of Trust Management Models

Dimension	Centralized Platform	Traditional Escrow	Permissionless Marketplace	BDTM Framework
Trust anchor	Platform reputation	Licensed intermediary	Cryptographic consensus	Cryptographic consensus + verified identity
Reputation portability	None (platform-specific)	None	Partial (chain-specific)	Full (DID-based)
Transaction transparency	Limited	Minimal	Full	Full (permissioned visibility)
Dispute resolution	Platform arbitration	Legal process	None (code is law)	Decentralized arbitration pool
Fraud detection	Internal algorithms	Manual review	Community vigilance	Automated + network auditing
Identity privacy	Platform-controlled	Required disclosure	Pseudonymous	Selective disclosure via ZKP
Regulatory compliance	Established	High	Uncertain	Configurable
Scalability (transactions/second)	High (10^4 – 10^5)	Low (manual)	Medium (10 – 10^3)	Medium (10^2 – 10^3 permissioned)
Cross-border suitability	High (platform-dependent)	Moderate	High	High
Operational cost structure	Transaction fees (2–15%)	Escrow fees (1–5%)	Gas fees (variable)	Protocol fees (low fixed)

It can be observed from the above comparative analysis that bdtm is situated at an intermediate point between centralized

systems and permission-less marketplaces. In fact, bdtm retains the performance and compliance strengths of permissioned blockchains while offering the benefits of transparency and portability offered by decentralization. Selective disclosure mechanism incorporated in bdtm resolves the issue of privacy faced by blockchain commerce due to transparency.

4. Operational Considerations and Limitations

Several issues need to be examined. Network effect becomes one of the major impediments to adoption as its value grows with more participants involved; however, initial participants will not see many benefits before the critical mass is reached. Possible strategies for dealing with the problem can be integration of the reputation network into already existing marketplaces as a reputation layer instead of the full replacement of the existing platform enabling sellers to develop their reputation and continue using the existing marketplace.

The scalability is still limited due to the permissioned blockchain approach. Even though hyperledger fabric significantly outperforms public blockchains, it may still be needed to shard or apply some other techniques to make the solution scalable if we want to achieve the same level of transactions as the big e-commerce platforms have.

However, regulatory uncertainty poses one of the greatest challenges. There is variation in terms of whether the chain-of-records will be legally recognized, and whether the award from a decentralized arbitration will be recognized under many laws. The configurability of the compliance component within the system enables jurisdiction-based rules to be set, but at the same time poses some risks.

V. CONCLUSION

In this research, the concept of the blockchain-enabled trust management framework for safe and transparent internet commerce is discussed. This framework combines decentralized identity verification, smart contract escrow, reputation scoring and decentralized dispute resolution into a unified design and offers trust verification that does not depend on any centralized intermediaries.

It is shown that blockchain-enabled trust management system possesses significant benefits in comparison with existing approaches in terms of transparency, fraud prevention and reputation portability. First of all, the immutable ledger makes it possible to conduct full-scale audit of the network. Secondly, smart contracts remove counterparty risk associated with payment versus delivery transactions. Finally, reputation based on did allows sellers to create portable trust record.



The comparative analysis puts bdtm into perspective as a hybrid mechanism that keeps the performance and compliance features of permissioned blockchain systems while delivering the transparency feature of a decentralized system. It is a consequence of the recognition that permissionless marketplaces are subject to certain limitations that limit their applicability and which can be addressed by permissioned mechanisms without losing trust-related benefits.

There are several limitations that restrict the practical use of this framework. The network effect works against new players, and the attainment of the required critical mass of participants presupposes some ways To use the current commerce infrastructure instead of competing with it. The scalability of bdtm is limited compared to the centralized systems and can be used only for high-volume consumer marketplaces.

Possible directions for future work include empirical evaluation via pilot implementations in borderless trade corridors, standardization of interoperable reputation measures to facilitate cross-chain mobility, and research into hybrid systems that would combine blockchain-enabled trust architecture with a centralized ui. The incorporation of zero-knowledge proofs in order to ensure anonymous reputation checks and the expansion of the system's scope to include agent-based commerce would be especially useful areas of further exploration.

Given the direction in which e-commerce is moving in terms of disintermediation, facilitated by the increasing regulatory pressure on platform monopolies, the progress in ai-assisted commerce, and customers' desire for data sovereignty, the development of blockchain trust architecture becomes increasingly plausible. The framework presented in this paper provides a solid basis for it.

commerce,” Decentralized Identity Foundation Position Statement, Mar. 2026.

REFERENCES

1. A. Sharma, R. Kumar, and S. Patel, “System Design and Practice of Blockchain Technology in Cross-Border E-Commerce Supply Chain Trust Management,” in Proc. IEEE Int. Conf. Advanced Computing and Communication, Indore, India, Dec. 2025, pp. 1–8.
2. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” *Applied Innovation Review*, vol. 2, pp. 6–19, 2016.
3. J. Dutta, A. Chowdhury, and S. Roy, “Smart Payment System: Blockchain-Powered Peer-to-Peer Transactions, Loans, and Fundraising,” in Proc. IEEE Int. Conf. Computing and Network Communications, Bangalore, India, Nov. 2025, pp. 1–6.
4. D. Hobbs, “From Agent-Visible to Agent-Actionable: KYA-OS, a Rail-Agnostic Trust Layer for E-commerce,” Decentralized Identity Foundation Position Statement, Mar. 2026.
5. L. Chen, M. Zhang, and K. Watanabe, “VisorFair: Bridging Reputation, Anonymity and Fairness in Decentralized Marketplaces,” in Proc. IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications, Dubrovnik, Croatia, Oct. 2025, pp. 1–10.
6. A. Rahmawati and B. Santoso, “The Role of Blockchain Technology in Enhancing Consumer Trust and Data Privacy Security on E-Commerce Platforms in Indonesia,” *Jurnal Sistem Informasi*, vol. 19, no. 2, pp. 45–58, 2024.
7. R. Gupta, S. Nair, and P. Singh, “Redefining Crowdfunding with Blockchain: Ethereum-based Smart Contract Implementation,” in Proc. IEEE Int. Conf. Blockchain and Cryptocurrency, Jan. 2026, pp. 1–7.
8. Y. Zhang, L. Wang, and H. Liu, “Decentralized Identity Management Based on Autonomous Identity in E-Commerce and Its Application to Key Opinion Leader,” in Proc. IET Int. Conf. Artificial Intelligence and Advanced Manufacturing, Dec. 2024, pp. 1–8.
9. V. Kumar, A. Mehta, and S. Iyer, “A Blockchain Based Reputation System for E-Commerce Protecting Vendor Identities and Data,” in Proc. IEEE Int. Conf. Recent Trends in Information Technology, Salem, India, Aug. 2025, pp. 1–7.
10. E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding,” in Proc. IEEE Symposium on Security and Privacy, 2018, pp. 583–598.