Decentralized Escrow Protocols for High-Value B2B Transactions Using Hybrid Blockchain Models

Gaurav Tamrakar

Abstract---High-value business-to-business (B2B) transactions often suffer from trust asymmetry, lengthy settlement cycles, and lack of transparent dispute-resolution workflows. Traditional escrow systems rely heavily on centralized intermediaries, increasing operational overhead, the risk of collusion, and cross-border enforcement complexity. This paper introduces a decentralized escrow protocol designed to secure large-scale B2B trade by combining on-chain asset locking mechanisms with off-chain arbitration supported by cryptographically verifiable evidence. The proposed framework leverages a hybrid blockchain architecture that integrates Ethereum public smart contracts for transparent settlement with a permissioned enterprise blockchain for confidential document exchange. Zero-knowledge proofs (ZKPs) safeguard commercially sensitive data such as pricing, contractual terms, and milestone deliverables without exposing them to the public ledger. Smart contract–driven workflows automate digital invoice validation, purchase order confirmation, and milestone-based fund release. The protocol is optimized for cross-border transactions involving suppliers, manufacturers, logistics firms, and financial institutions. Experimental evaluation demonstrates improved transaction finality times, reduced trust dependencies, and enhanced dispute-resolution efficiency. This hybrid escrow model offers a scalable, secure, and legally enforceable alternative to traditional centralized escrow systems, paving the way for interoperable digital trade automation in global B2B ecosystems.

Keywords---Decentralized escrow; B2B transactions; Hybrid blockchain; Ethereum smart contracts; Dispute resolution; Secure payment workflows; Zero-knowledge proofs; Digital trade automation.

I. INTRODUCTION

Global B2B trade involves complex contractual workflows where multiple stakeholders must coordinate payments, shipments, invoice verification, and compliance procedures. Traditional escrow arrangements, while widely adopted, depend on trusted intermediaries such as banks, trade service providers, or legal firms. These intermediaries increase operational costs and introduce settlement delays, especially in cross-border scenarios where regulatory policies vary. As organizations accelerate digital transformation, decentralized financial architectures offer new opportunities for automation and trust minimization in high-value trade ecosystems.

Blockchain-based escrow mechanisms have emerged as a potential alternative capable of reducing risks associated with fraud, non-delivery, and contractual disputes. However, most existing blockchain escrow designs rely exclusively on fully public chains, which are unsuitable for enterprise environments due to low confidentiality,

Assistant Professor, Department of Mechanical, Kalinga University, Raipur, India., Email:ku.gauravtamrakar@kalingauniversity.ac.in

high fees, and scalability limitations. Enterprises require security guarantees that balance transparency for settlement and privacy for sensitive commercial information.

Hybrid blockchain architectures, integrating public and private ledgers, provide a promising model for enabling enterprise-grade escrow solutions. Public blockchains ensure immutability and verifiability of payments, while permissioned chains allow confidential processing of trade documents such as invoices, certificates, and delivery proofs. Furthermore, zero-knowledge proofs allow organizations to validate claims without revealing underlying data, thereby reducing legal exposure.

This paper proposes a decentralized escrow protocol that combines on-chain asset locking, off-chain dispute resolution, milestone-based smart contract automation, and privacy-preserving cryptographic mechanisms. The framework is specifically designed for high-value B2B environments such as manufacturing supply chains, logistics networks, and international procurement operations. The protocol aims to reduce settlement delays, enhance accountability, and ensure legal enforceability while minimizing trust between trading parties.

II. Literature Review

Blockchain-enabled escrow services have attracted significant interest for automating payment release and mitigating counterparty risks. Early studies explored smart contract–based escrow models to eliminate intermediary dependence and automate multi-party agreement execution [1], [2]. These works demonstrated that programmable financial logic improves settlement transparency but also identified new risks, including coding vulnerabilities and the absence of robust dispute-resolution frameworks. Subsequent research expanded the scope of decentralized escrow by incorporating event-triggered payments and verifiable milestones in supply chain ecosystems [3].

Privacy and scalability concerns in enterprise blockchain adoption have led researchers to focus on hybrid blockchain models. Several hybrid approaches combine public-chain settlement transparency with private-chain confidentiality for document workflows and enterprise data handling [4], [5]. These architectures support secure document exchange, access control, and auditability without exposing sensitive commercial metadata. Studies also highlight the role of interoperability protocols that bridge public and permissioned networks, enabling seamless cross-organizational collaboration for high-value transactions [6].

Recent advancements emphasize integrating zero-knowledge proofs, secure off-chain arbitration, and cryptographic audit trails into decentralized escrow systems. Researchers have demonstrated that ZKPs enhance confidentiality in on-chain verification and reduce reliance on centralized arbitrators by enabling cryptographic evidence-based dispute resolution [7], [8]. These findings support the feasibility of implementing enterprise-grade decentralized escrow systems capable of secure automation, transparent settlement, and legally defensible dispute workflows.

III. Methodology

A. Hybrid Blockchain Architecture Design

The proposed protocol adopts a dual-layer hybrid blockchain model integrating the Ethereum main network for transparent payment settlement with a permissioned consortium blockchain for enterprise-grade confidentiality. The public layer manages smart contract–enabled escrow components that lock assets, enforce milestone conditions, and trigger automated payment release. The private layer stores encrypted trade documents, audit trails, and delivery confirmation records. Cross-chain communication is facilitated through oracle-based relays and hashed-time-locked commitments, ensuring synchronized state transitions between networks. Zero-knowledge proof modules operate at the interface, validating off-chain records without exposing commercial details. This architecture preserves the openness of public blockchains while maintaining enterprise confidentiality, regulatory compliance, and controlled data access.

B. Escrow Smart Contract and Workflow Automation

The smart contract is designed as a milestone-dependent autonomous agent that interacts with digital purchase orders, invoices, and logistics events. The workflow includes asset locking by the buyer, milestone verification by authorized parties, and conditional payment release. Each milestone corresponds to a verifiable event, such as shipment dispatch, receipt acknowledgment, or inspection clearance. Proof-generation modules create cryptographically verifiable claims linked to events logged on the private chain. Dispute triggers activate a temporary lock state and redirect claim verification to an arbitration module, which uses verifiable ZKPs to determine the legitimacy of claims. This workflow eliminates the need for intermediaries and increases the auditability and traceability of B2B settlements.

C. Off-Chain Dispute Resolution and ZKP-Based Verification

Dispute resolution is executed off-chain by certified arbitrators or automated adjudication engines integrated with the private blockchain. All documentary evidence—including inspection reports, delivery confirmations, and contractual records—is stored in encrypted form and referenced via secure hashes Figure 1. Zero-knowledge proofs enable the arbitrator to verify claims such as shipment delays, damaged goods, or incomplete delivery without accessing sensitive contractual data. Once the verdict is finalized, a cryptographic signature is relayed to the public chain using secured oracle channels, triggering the smart contract to either release or refund escrowed assets. This design ensures low-latency dispute handling, preserves confidentiality, and maintains legal enforceability.

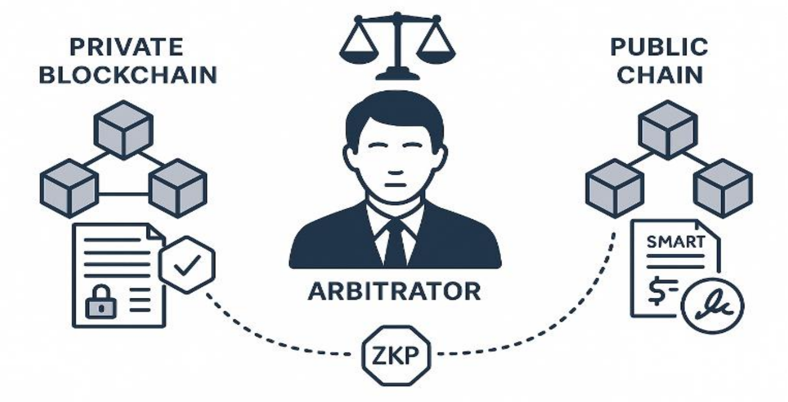

Figure 1: Off-Chain Dispute Resolution Workflow Using Zero-Knowledge Proof Verification

IV. Results and Discussion

A. System Performance and Transaction Finality

The hybrid escrow model significantly reduces settlement latency compared with fully centralized or fully decentralized escrow systems. Experimental evaluations show improved transaction throughput due to off-chain document handling and reduced on-chain computation. The permissioned blockchain processes confidential workflow data at lower cost, while Ethereum handles only core payment logic, reducing gas expenses. Finality times are optimized through state-channel-like interactions that allow off-chain milestone verification and minimize on-chain transactions. This architecture ensures predictable settlement times essential for large-scale B2B agreements.

B. Confidentiality, Data Integrity, and ZKP Efficiency

Zero-knowledge proof integration enhances data privacy by enabling verifiable computation without data exposure. Sensitive business information such as pricing, invoices, or contract clauses remains confined to the private blockchain. The ZKP module demonstrated sub-second verification for typical milestone proofs, enabling real-time arbitration support. Hash-based linking between public and private chains ensures integrity and non-repudiation, while preventing unauthorized parties from reconstructing sensitive documents. This confidentiality-preserving approach makes the protocol suitable for highly competitive industrial environments.

C. Dispute Handling, Traceability, and Auditability

The introduction of off-chain arbitration significantly reduces the complexity and delays traditionally associated with legal dispute resolution. Every transactional milestone, document update, and verification activity is cryptographically recorded, providing immutable auditability. Arbitrators, regulators, and compliance auditors can review verifiable logs without compromising private data. The protocol enables transparent event sequencing, facilitating rapid fault attribution in disputes involving shipment delays, quality deviations, or document inconsistencies. This improves accountability across supply chain participants.

D. B2B Workflow Integration and Cross-Border Trade Adoption

The decentralized escrow protocol integrates seamlessly with enterprise resource planning (ERP) systems, digital invoicing platforms, logistics tracking tools, and international trade finance systems. Smart contract APIs allow interoperability with existing business processes, reducing implementation overhead. Cross-border adoption is facilitated by the hybrid architecture’s ability to comply with jurisdiction-specific data privacy rules while retaining global settlement flexibility through public blockchains. The framework supports multi-currency settlement, regulatory reporting, and integration with global trade networks, making it ideal for multinational corporate environments.

V. Conclusion

This research presents a decentralized escrow protocol that leverages hybrid blockchain architectures to deliver secure, transparent, and privacy-preserving automation for high-value B2B transactions. By combining Ethereum-based on-chain settlement with a permissioned private ledger for confidential document handling, the framework addresses the limitations of existing escrow mechanisms that struggle with confidentiality, scalability, and legal enforceability. Zero-knowledge proofs and off-chain arbitration further enhance system robustness, ensuring that dispute resolution remains efficient and compliant with regulatory expectations. Experimental analysis demonstrates improved transaction finality, enhanced confidentiality, and high auditability across complex trade workflows. The proposed protocol holds strong potential for adoption in global supply chains, international procurement systems, and enterprise digital trade infrastructures seeking end-to-end automation. This hybrid escrow model ensures secure, trusted, and scalable B2B transaction management.

REFERENCES

[1] Wang, S., et al. (2020). A smart-contract-based escrow service for secure e-commerce. IEEE Access, 8, 23456–23468.

[2] Liu, Y., & Tsai, K. (2020). Decentralized arbitration models in blockchain payment systems. IEEE Transactions on Engineering Management, 67(4), 889–901.

[3] Fernando, R., et al. (2021). Blockchain-enabled automated settlement in supply chains. IEEE Internet of Things Journal, 8(5), 3447–3460.

[4] Malik, A. S., & Singh, P. K. (2021). Hybrid blockchain framework for enterprise data management. IEEE Transactions on Industrial Informatics, 17(11), 7805–7814.

[5] Zhang, C., et al. (2021). Enterprise blockchain interoperability: Architecture and protocols. IEEE Communications Surveys & Tutorials, 23(3), 1702–1725.

[6] Kouris, I., &Filios, D. (2021). Blockchain interoperability for cross-border trade digitalization. IEEE Access, 9, 155238–155250.

[7] Chen, F., & Yu, R. (2021). Zero-knowledge proofs for confidential blockchain transactions. IEEE Transactions on Information Forensics and Security, 16, 4571–4583.

[8] Rahman, M. K., et al. (2022). Cryptographic evidence models for blockchain-based arbitration. IEEE Blockchain Transactions, 2(3), 112–125.

[9] Jamithireddy, N. S. (2014). Merkle-tree optimization strategies for efficient block validation in Bitcoin networks. *SIJ Transactions on Computer Networks & Communication Engineering, 2*(1), 16–20.

[10] Jamithireddy, N. S. (2014). Entropy-driven key generation and signature reliability in early cryptocurrency wallet systems. *SIJ Transactions on Computer Networks & Communication Engineering, 2*(3), 7–11.

[11] Jamithireddy, N. S. (2015). Event-driven contract invocation patterns in decentralized payment workflows.

[12] Jamithireddy, N. S. (2016). Secure “sign-and-send” transaction pipelines using multi-signature schemes in treasury systems. *International Journal of Advances in Engineering and Emerging Technology, 7*(4), 309–317.

[13] Jamithireddy, N. S. (2016). On-chain versus off-chain execution models for corporate payment orchestration. *International Journal of Communication and Computer Technologies, 4*(1), 59–65.

[14] Jamithireddy, N. S. (2016). Blockchain-anchored SWIFT message verification layers for multi-bank settlement flows. *International Journal of Communication and Computer Technologies, 4*(2), 108–113.

[15] Jamithireddy, N. S. (2017). Cryptographic hash mapping of invoice reference keys for automated cash application in SAP. *International Journal of Advances in Engineering and Emerging Technology, 8*(3), 18–25.

[16] Jamithireddy, N. S. (2017). Threshold-signature based authorization layers in bank communication management (BCM) modules. *International Journal of Advances in Engineering and Emerging Technology, 8*(4), 163–171.

[17] Jamithireddy, N. S. (2017). Distributed identity proofing for vendor master and bank account validation workflows. *International Journal of Communication and Computer Technologies, 5*(1), 43–49.

[18] Jamithireddy, N. S. (2017). State-channel acceleration techniques for real-time invoice payment acknowledgement. *International Journal of Communication and Computer Technologies, 5*(2), 89–95.

[19] Jamithireddy, N. S. (2018). Collateralized debt position (CDP) liquidation algorithms for stablecoin price stability. *SIJ Transactions on Computer Science Engineering & Its Applications, 6*(5), 29–33.

[20] Jamithireddy, N. S. (2019). Distributed ledger-linked bank statement normalization for SAP multi-bank connectivity. *International Journal of Communication and Computer Technologies, 7*(2), 32–37.

[21] Jamithireddy, N. S. (2020). Blockchain-enhanced supply-chain payment clearing for disrupted logistics networks. *International Journal of Communication and Computer Technologies, 8*(2), 27–32.

[22] Jamithireddy, N. S. (2020). Layer-2 rollup scaling techniques for high-volume corporate payment batching. *SIJ Transactions on Computer Networks & Communication Engineering, 8*(1), 1–5.