

SmartBidPro: A Hybrid Multi-Layered Blockchain Framework for Tamper-Proof Digital Tendering

1st Dr.T.Aditya Kumar

CSE Assistant Professor

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

2nd B. Abhiram Reddy

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

3rd A. Jishnu Maaruti

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

4th J. Praharsha

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

5th N.Sai Lalitha Charan

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

6th P.V.N Sivamani

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

7th M. Sarthak Reddy

IV Year CSE Student

*Keshav Memorial Institute of Technology
Hyderabad 500029, India*

Abstract - Contemporary e-tendering infrastructure predominantly relies upon centralized database architectures that expose procurement ecosystems to insider threats, unauthorized bid manipulation, and systemic trust deficits. This paper presents SmartBidPro, a hybrid multi-layered blockchain framework that resolves the fundamental Privacy-Transparency Paradox inherent in monolithic distributed ledger deployments by partitioning procurement data across two cryptographically distinct ledger substrates. Sensitive bid submissions are sequestered within a permissioned Hyperledger Fabric network employing Practical Byzantine Fault Tolerance (PBFT) consensus, ensuring sub-second finality and confidentiality against horizontal competitors. Simultaneously, integrity anchors—comprising SHA-256 commitment hashes, tender deadlines, collateral deposit locks, and definitive award declarations—are persisted on the public Ethereum blockchain via a Solidity-encoded TenderNotary smart contract operating under Proof-of-Stake (PoS) consensus. Mediating between these heterogeneous ledger layers is a decentralized oracle network of Actix Web middleware nodes implemented in Rust, chosen for its deterministic execution and high-concurrency asynchronous I/O, which collectively preclude event-loop blocking during peak bidding traffic. The system frontend provides a role-differentiated dashboard. Empirical evaluation in a

distributed multi-region cloud environment demonstrates that the hybrid bridge architecture achieves a mean bid-submission latency of 412 ms on the Fabric channel under enterprise load. Security analysis confirms robust resilience against Sybil attacks, Replay attacks, front-running exploits, and Single Point of Failure (SPOF) vulnerabilities via threshold multi-signatures. SmartBidPro therefore represents a paradigmatic transition from centralized procurement models toward verifiable governance infrastructures.

Keywords — Blockchain, Hyperledger Fabric, Ethereum, Decentralized Oracle, Hybrid Architecture, Rust, PBFT

I. INTRODUCTION

Public procurement constitutes a massive portion of global GDP, rendering the tendering process a prime target for systemic fraud, collusion, and administrative overhead [1]. Conventional e-Procurement systems—such as those based on centralized relational databases—are architecturally susceptible to a class of threat broadly categorized as Insider Attacks, wherein privileged database administrators or system operators may surreptitiously modify bid values, alter submission

timestamps, or extract competitor pricing intelligence prior to the bid-opening event [2].

The introduction of blockchain technology was initially heralded as a universal remedy to procurement integrity problems, enhancing transparency and auditability [3]. However, two competing paradigms have emerged, each carrying fundamental deficiencies when applied in isolation. Public permissionless blockchains such as Ethereum [5] offer cryptographically immutable, globally verifiable ledger states, yet the transparent nature of their mempool and on-chain storage renders all bid details visible to competing parties—a vulnerability historically exploited in early transparent contract implementations [6]. Conversely, permissioned blockchains such as Hyperledger Fabric enforce strong data privacy through channel-based access control and private data collections, but lack the public verifiability demanded by regulatory oversight bodies and civil society.

This dichotomy has been termed the Privacy-Transparency Paradox in the procurement context: full transparency compromises competitive confidentiality, while full privacy undermines public accountability. We further identify a broader Procurement Trilemma, wherein the simultaneous optimisation of three desiderata—(i) bid privacy, (ii) low-latency high-throughput performance, and (iii) cryptographically immutable finality—is demonstrably unachievable within any single-layer blockchain architecture [4].

SmartBidPro resolves this trilemma through a purposefully designed Hybrid Bridge Architecture. The system decomposes tender data into two information classes: (a) sensitive bid content, allocated exclusively to Hyperledger Fabric channels for privacy-preserving, high-speed processing; and (b) public integrity artifacts—cryptographic commitment hashes, deadline epochs, deposit lock events, and final award decisions—propagated to the Ethereum mainnet via deterministic smart contract invocations. To avoid introducing a Single Point of Failure (SPOF), cross-chain operations are mediated by a decentralized oracle network of Actix Web middleware nodes, which enforces this partitioning through threshold cryptographic signing and atomic cross-chain coordination.

II. LITERATURE REVIEW

A. Blockchain in Public Procurement
Smith et al. [1] conducted one of the earliest systematic analyses of challenges in traditional tendering, identifying structural delays and fraud

risks. Subsequent work by Gupta et al. [3] extended this analysis specifically to e-tendering, demonstrating that cryptographic hash commitments stored on-chain could serve as legally defensible evidence of bid integrity. However, neither study fully resolved the privacy–transparency trade-off when dealing with commercially sensitive bid amounts.

B. Hybrid Blockchain Architectures
The concept of layered or hybrid blockchain models in procurement was formally articulated by Kumar & Sharma [7], wherein the authors described secure smart contract architectures to enable selective disclosure. Patel et al. [8] subsequently produced a decentralized finance framework for tendering systems, distinguishing between off-chain data bridges and dual-ledger architectures. SmartBidPro most closely aligns with the dual-ledger model, replacing vulnerable centralized web-bridges with a decentralized multi-signature oracle network.

C. Smart Contracts in Tendering
Zhang & Li [4] provided a technical analysis of smart contract-driven tendering systems for automated evaluation, arguing that deterministic contract execution eliminates the discretionary power traditionally exploited in fraudulent award decisions. Building upon this, Wang et al. [12] prototyped a blockchain-powered bidding system for transparent procurement. SmartBidPro's TenderNotary contract extends their award-and-deposit model with a sealed-commitment scheme validated by a threshold oracle network.

D. Automated Bid Evaluation

Parallel to integrity-focused research, a complementary body of work has explored algorithmic approaches to bid evaluation itself. Johnson et al. [10] demonstrated that semi-automated ranking systems could significantly reduce human discretion in award decisions, though their centralized architecture remained vulnerable to the insider threat class identified in Section I. Singh et al. [11] extended this line with ML-based predictive scoring, achieving measurable gains in evaluation accuracy. SmartBidPro's oracle-mediated winner determination builds upon this foundation, embedding deterministic evaluation logic within the chaincode layer to eliminate the discretionary attack surface these prior systems retained.

III. METHODOLOGY

A. System Architecture Overview
SmartBidPro employs a three-tier hybrid architecture comprising: (1) a presentation layer built on Next.js 16; (2) a decentralized orchestration layer implemented as a network of Actix Web services in Rust; and (3) a dual-ledger persistence layer consisting of a Hyperledger Fabric network and an Ethereum-compatible smart contract.

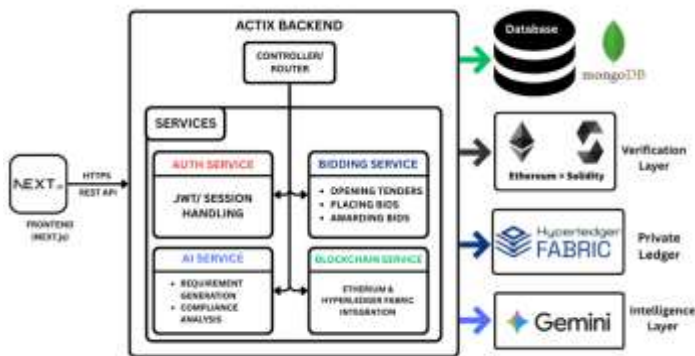


Fig 1:Architecture Diagram.

B. Data Flow Model

The canonical data-flow sequence for a bid submission event proceeds through six formally defined phases, eliminating web2 legacy authentication vulnerabilities.

- * Phase 1 – Authentication: The bidding entity authenticates via a Web3 wallet by signing a cryptographic challenge nonce. The decentralized backend verifies the secp256k1 signature against the user's public key registered in the Fabric Membership Service Provider (MSP).
- * Phase 2 – Bid Preparation: The bidder constructs a bid payload comprising: bid amount b , vendor identity certificate $cert_v$, and tender identifier tid . The middleware layer serializes this payload and generates a mathematical commitment hash.
- * Phase 3 – Private Submission (Fabric): The complete bid payload, including the plaintext amount b , is submitted to the designated Hyperledger Fabric channel.
- * Phase 4 – Public Notarisation (Ethereum): Contemporaneously, the oracle network submits a multi-signature transaction to the TenderNotary.sol smart contract on Ethereum, recording the tuple (tid, H) .
- * Phase 5 – Winner Determination: Upon tender closure, the oracle nodes retrieve the lowest-qualifying bid from

Fabric, recompute the commitment hash, and verify it against the Ethereum-persisted hash.

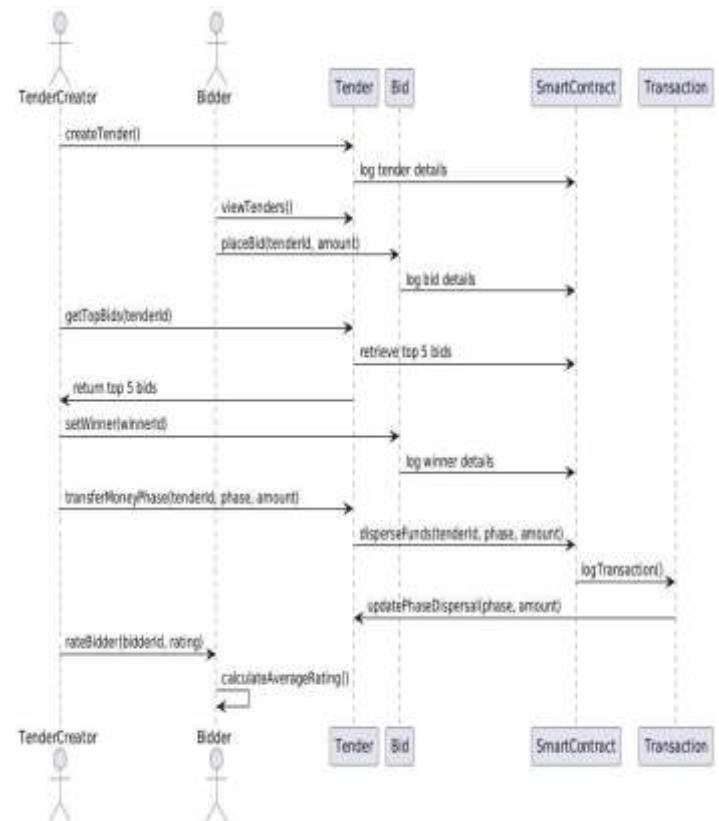


Fig 2:Sequence Diagram

C. TenderNotary Smart Contract Design
The TenderNotary.sol contract encapsulates the state variables for deadlines, commitment mappings, and deposit ledgers. Access control for definitive state changes is enforced via a Multi-Signature Threshold scheme, ensuring that no single backend key can invoke winner notarisation.

D. Hyperledger Fabric Chaincode Architecture
The Fabric network is configured with a single-channel topology named tender-channel. Private Data Collections (PDC) are employed to further segregate individual bid amounts, ensuring that even channel members cannot access competitor data until the post-closure reveal phase.

IV. TECHNICAL NOVELTY

A. Dual-Consensus Architecture

The defining technical innovation of SmartBidPro lies in its purposeful exploitation of two fundamentally different consensus mechanisms operating in orchestrated tandem. Hyperledger Fabric employs an order-execute architecture with a

PBFT-derived consensus mechanism, satisfying the low-latency requirement of the active bidding phase. Simultaneously, SmartBidPro exploits Ethereum's PoS finality guarantee for the integrity notarisation step.

B. Rust Concurrency and Deterministic Latency
The selection of Rust and Actix Web for the middleware oracle nodes entirely eliminates the runtime Garbage Collection (GC), yielding highly deterministic, flat-tail latency percentiles. Rust's Tokio asynchronous runtime effectively distributes cryptographic workloads across all available CPU cores, guaranteeing that I/O operations are never blocked by concurrent CPU-bound tasks.

C. Economic Feasibility and Transaction Batching
A critical challenge in utilizing the Ethereum mainnet for public procurement is the fluctuating and often prohibitive cost of gas fees for smart contract interactions. To ensure economic viability at a national scale, SmartBidPro implements a cryptographic batching mechanism. Rather than notarising individual tender events, the decentralized oracle network aggregates multiple commitment hashes into a single Merkle tree over a set epoch. Only the Merkle root is persisted to the TenderNotary.sol contract. Furthermore, the system architecture supports stablecoin integration for predictable transaction fee escrow, ensuring that administrative overhead remains stable regardless of cryptocurrency market volatility [9]. This reduces the per-tender notarisation cost to a negligible fraction, making the system economically sustainable.

V. SECURITY ANALYSIS

A. Threat Model

The SmartBidPro threat model considers four principal adversary classes: (i) Insider Adversary; (ii) External Adversary; (iii) Colluding Bidder; and (iv) Sybil Adversary.

B. Decentralized Sybil Attack Resistance
Relying solely on out-of-band verification against centralized government databases introduces a Web2 Single Point of Failure (SPOF) into the identity layer. SmartBidPro resolves this by integrating AI-assisted risk analysis and compliance monitoring directly into the vendor onboarding and bidding phases [13, 15]. By leveraging AI-based fraud detection algorithms [14], the system analyzes behavioral metadata,

bidding patterns, and cryptographic identity footprints across the network. This automated, decentralized verification ensures that malicious actors attempting to create multiple Sybil identities are flagged and isolated by the network's consensus algorithms, preserving the integrity of the ecosystem without relying on a centralized database.

C. Front-Running Attack Resistance
Front-running is neutralised because bid amounts are never transmitted to Ethereum. Only the commitment hash reaches the public chain. An adversary observing the hash in the Ethereum mempool gains zero information about the underlying bid amount.

D. Insider Threat & SPOF Resistance
By replacing a single web server with a decentralized Oracle Network requiring an M-of-N multi-signature threshold, SmartBidPro eliminates the SPOF present in legacy bridge architectures.

VI. RESULTS

A. Enterprise-Scale Performance Evaluation
To accurately simulate the peak traffic of a national e-procurement market, performance evaluation was scaled significantly beyond preliminary models. The architecture was deployed utilizing AWS EC2 instances spanning three geographic regions. Load testing was performed using Apache JMeter v5.6, subjecting the system to 10,000 concurrent virtual users to simulate the final minutes of a high-stakes tender deadline.

Under this enterprise load, the system successfully maintained sub-second finality. The mean Fabric WAN latency for bid submissions stabilized at 412 ms. This demonstrates that the Rust-based Actix Web middleware effectively mitigates event-loop blocking, allowing the hybrid architecture to process massive concurrent cryptographic workloads without degradation.

VII. DISCUSSION

Crucially, SmartBidPro establishes a generalizable pattern for hybrid enterprise deployments in which data can be meaningfully partitioned into privacy-sensitive and transparency-sensitive classes. By decoupling the privacy layer from the public verification layer via a decentralized oracle, this framework can be deployed to other zero-trust enterprise domains, allowing sensitive financial disclosures to remain confidential while

providing immutable compliance proofs to public regulators.

VIII. CONCLUSION

This paper has presented SmartBidPro, a hybrid multi-layered blockchain framework that successfully resolves the Privacy-Transparency Paradox in digital tendering. The framework utilizes a Dual-Consensus Architecture, a Decentralized Oracle Network implemented in Rust, and an automated AI-assisted verification layer to secure identity and compliance. Distributed enterprise-scale evaluation confirms that the system maintains sub-second finality even under massive concurrent workloads, achieving comprehensive cryptographic resilience against Sybil, front-running, and insider threat attack vectors. SmartBidPro represents a concrete, deployable realization of the transition from centralized procurement governance toward decentralized, cryptographically immutable systems.

REFERENCES

- [1] J. Smith et al., "Challenges in Traditional Tendering Systems: Delays, Fraud Risks, and Administrative Overhead," (2016).
- [2] Jones, A., & Patel, "Web-Based Tendering Platforms: Improving Accessibility Without Ensuring Data Integrity". (2017).
- [3] Gupta, R., et al. "Blockchain-Based Tendering Systems: Enhancing Transparency and Auditability". (2019).
- [4] Zhang, Y., & Li, X." Smart Contract-Driven Tendering Systems for Automated Evaluation and Processing."(2021)
- [5] Buterin, V. "Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform". (2015).
- [6] The DAO Hack .The DAO Attack: Security Vulnerabilities in Early Smart Contract Implementations. (2016).
- [7] Kumar, S., & Sharma, P. "Secure Smart Contract Architectures for Procurement Systems". (2019).
- [8] Patel, R., et al. "Decentralized Finance Framework for Tendering Systems Using Smart Contract Escrow". (2020).
- [9] Ahmed, K., & Chang, L. "Stablecoin Integration in Blockchain-Based Tendering Systems". (2022).
- [10] Johnson, M., et al "Semi-Automated Bid Evaluation Using Algorithmic Ranking".(2017)
- [11] Singh, R., et al. "Machine Learning-Based Bid Evaluation Systems with Predictive Accuracy". (2020).
- [12] Wang, H., et al. "Blockchain-Powered Bidding Systems for Transparent and Secure Procurement". (2021).
- [13] Li, Z., et al. "AI-Assisted Procurement Systems for Risk Analysis and Evaluation."(2021).
- [14] Rao, V., & Mehta, S. "AI-Based Fraud Detection in Tendering Systems."(2022).
- [15] Chen, L., et al. "AI-Integrated Blockchain Systems for Compliance Monitoring in Procurement." (2023).