International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V4I2P112
Eureka Vision Publication | Volume 4, Issue 2, 121-130, 2023

Original Article

Blockchain and Smart Contracts in Claims Settlement

Komal Manohar Tekale[1], Nivedita Rahul[2]
[1,2] Independent Researcher, USA.

Abstract - In this paper, a model is presented in the operational form of blockchain and smart contract utilization to modernise insurance claims settlement, which is enterprise-ready. Design a permissioned, Ethereum-compatible ledger that encodes policy terms limits, deductibles, exclusions and orchestrates deterministic claim state transitions from First Notice of Loss (FNOL) to payout. Off-chain storage stores sensitive artifacts (PII/PHI, images, medical records) encrypted in vaults, and on-chain records append cryptographic digests and events that can be audited by tampering evidence. This is provided by evidence (in the form of signed oracles, such as weather indices, hospital discharge summaries, police reports), and permits parametric claims to be settled quickly and routine indemnity claims to undergo high straight-through processing (STP) with human attention reserved to exceptions. The methodology emphasizes formal assurance (static analysis, property-based tests, optional formal verification), runtime safety (circuit breakers, timelocked upgrades), and robust key/oracle governance. Pilot testing in pilot testing, the methodology provides a shorter cycle time, less reconciliation, and quantifiable mitigation of fraud-leakage but still ensures regulatory compliance by selective disclosure and privacy-by-design. Also work through the dynamics of constraints throughput and fee dynamics, legal enforceability, legacy interoperability, and privacy-versus-transparency trade-off and a roadmap of staged adoption, starting with low-dispute, oracle-rich products, then triage, partial advances, and subrogation workflows. Findings indicate that blockchain is likely to be the most useful as a coordination/assurance layer to supplement, but not to substitute, fundamental insurance infrastructure.

Keywords - Blockchain, Smart contracts, Insurance claims, Claims settlement, zero-knowledge proofs, selective disclosure, privacy-by-design, interoperability.

1. Introduction

Insurance claims settlement continues to be one of the most complicated and most examined actions in the industry which is often crippled due to disjointed data, manual handling, and asymmetric information among carriers, intermediaries and policyholders. [1-3] The legacy processes that cover First Notice of Loss (FNOL), coverage checks, damage estimation, fraud investigations, and payment are usually based on segregated systems and batch reconciliation that extend cycle times and increase the cost of loss adjustment. Policy interpretation and documentation frustrations also disrupt the confidence of customers and escalate the operational risk. In the quest by insurers to achieve straight-through processing and real-time assurance, there is the increasing demand of infrastructure capable of delivering tamper-evident audit trails, deterministic business logic, and secure data exchange across organizational boundaries.

Blockchain and smart contracts offer a programmable substrate to address these pain points. Claim events can be shared among the stakeholders on a single source of truth on a permissioned ledger and access controls and privacy can be enforced. Smart contracts store policy terms restrictions, deductibles, exclusions and automatically consider the evidence presented by external oracles, such as FNOL systems, assessor reports, telematics and IoT sensors. On-chain Parametric designs (e.g. wind speed, flight delay, water level) are a parametric design, meaning their payout depends on pre-defined triggers, making them well-suited to be executed on-chain and disbursed on a rapid and low-dispute basis.

The use of complementary methods like zero-knowledge proofs and selective disclosure reduces the threat of exposing individual or proprietary data to common infrastructures to an excessive degree. In the following paper, blockchain-enabling claims are placed in the context of the digital transformation of the insurance industry, representing a description of a data architecture supporting the transition between core policy administration, data lakes, and analytics platforms to ledger-based adjudicated claims. Describe the ways of adoption of the pilot parametric products to automated indemnity claim triage and indemnity claim governance (formal verification, kill-switches, and runtime monitoring). Suggest metrics of evaluation cycle time, exception rate, straight-through processing, rate of dispute, and customer NPS to determine the existence of real operational and customer-experience benefits with claims settlement using smart contracts.

2. Literature Review

2.1. Existing Insurance Claim Settlement Models

Conventional claims processes generally follow a sequence of steps which includes First Notice of Loss (FNOL), confirmation of coverage, checking liability and loss, subrogation, and authorizing payments. Latency and error opportunity is introduced in each administration of handoff policies, [4-6] underwriting, TPAs, surveyors/assessors, and finance. In India, life insurers report high death-claim settlement ratios (around the high-90% range in 2022-23), yet cycle times and customer experience still vary widely across product lines. Motor and health claims usually take a cashless or reimbursement route: the former is based on network provider and pre-authorization regulations, and the latter is based on completeness of documents and post-facto examination. They both are sensitive to the quality of documentation, information asymmetry, and risk of fraud.

To mitigate delays, carriers have layered in process re-engineering and digitization: e-KYC, e-signatures, image-based damage assessment, and standardized discharge forms. Repetitive validations (policy status, premium dues, coverage limits), and claims triage based on complexity and fraud propensity have been taken over by Robotic Process Automation (RPA) now. Straight-Through Processing (STP) is being more aimed at the low-complex, high-volume claims, whilst complex cases are sent to expert adjusters with decision support. In spite of these, heterogeneous data across legacy cores, manual evidence collection and reconciliation overheads continue to impair end-to-end timeliness, raise loss adjustment cost and lower Net Promoter Scores (NPS).

2.2. Blockchain Adoption in Financial and Insurance Sectors

In financial services, blockchain has been tried in payments, trade finance, asset tokenization, and KYC utilities, insurance taking up many of the same primitives: shared ledgers to reconcile bordereaux, parametric risk triggers, and proof-of-process audit trail. Insurance Investment in blockchain insurance to ease enterprise experimentation has increased, and permissioned networks where privacy is maintained and multi-party coordination is possible are of interest in 2023. The general trend in Northern American insurers and reinsurers is the trend to lead proof-of-concepts, whereas Asia-Pacific is led by the agenda of digital transformation and regulation sandboxing.

The value thesis centers on three attributes: (i) immutability and time-stamped provenance to deter tampering; (ii) a single, synchronized data plane that reduces reconciliation; and (iii) programmable trust via smart contracts. These attributes are especially desirable in multi-stakeholder processes coinsurance, reinsurance placements and catastrophe response in which records are misaligned and delayed confirmations contribute to operational risk. However, it is blocked by the complexity of integrating it with legacy cores, privacy and confidentiality needs, throughput limitations compared to batch processing, and the necessity to have strong governance (onboarding rules, key management, change control). With increasingly sophisticated standards, privacy-protective procedures, insurers are increasingly seeing blockchain as a coordination layer, not as a wholesale substitute, to the existing data platform on the cloud and the existing analytic estates.

2.3 Smart Contract Mechanisms and Applications

Smart contracts represent a coverage limit of the business rules, deductibles, waiting periods in the form of deterministic code that is executed by the blockchain under predetermined conditions. They may have (a) policy validation (e.g. police FIR on motor theft, hospital discharge summary on health, meteorological data on parametric covers), (b) checking trigger conditions through oracles (e.g. police FIR on motor theft, hospital discharge summary on health) and (c) authorizing disbursement or route exceptions, in claims. The parametric insurance is an actual example of the fit, in this case, external index (wind speed, rainfall, flight delay, seismic intensity) exceeding a limit, the payout is calculated and discharged without loss adjustment subjectivity, minimizing dispute and cycle time.

Even in a case of indemnity claim in which the loss quantification is fine-tuned, smart contracts are still valuable to automate the processes of triage, reserving, part advancements and subrogation splits, and maintain a tamper-evident audit trail. Privacy is addressed through permissioned ledgers, off-chain data vaults, and selective disclosure; zero-knowledge proofs can attest to conditions (e.g., "deductible met") without exposing raw PHI/PII. The main issue under consideration is the oracle problem: the inputs of evidence have to be reliable, accessible, and non- manipulable; useful designs are thus a combination of cryptographically signed data feeds, attested middleware and multi-source quorum logic.

To implement smart contracts, software assurance Static analysis, Unit/property tests, and, to a high level, formal verification and runtime controls (circuit breakers, pause/upgrade paths, and key rotation) are all needed. Smart contracts can also be used to lift Straight-Through Processing of common claims, reduce exception queues and enhance transparency to policyholders and regulators, when combined with fraud analytics and case-management systems, using API gateways, and open the door to more scalable, more secure, and more customer-friendly products.

3. System Design and Architecture

The architecture illustrates a full-fledged claims journey throughout four domains: Policyholder and Frontend, Insurance Provider domain, Blockchain Layer, and Oracles and Integrations. The policyholder is through a mobile application or claims portal where FNOL details and documents are provided. [7-10] this submission is sent to the Claims Processor of the insurer which archives the complete record off-chain in the Claims DB but constructs a smaller claim hash and metadata to be anchored on-chain. Such a division maintains the privacy of sensitive data but gives an irrevocable reference to the set of evidence. Therein, the coordination of workflow happens through supporting services within the boundary of the insurer. The Notification Service presents the status updates to the claimant on occurrence of an event by the smart contract (such as claim created, triaged, or settled). A non-compulsory KYC/Identity Service is able to answer on-chain queries with attestations, which means identity or eligibility checks can be proved without revealing raw PII. The contract refers to these attestations although the data behind them is off-chain.

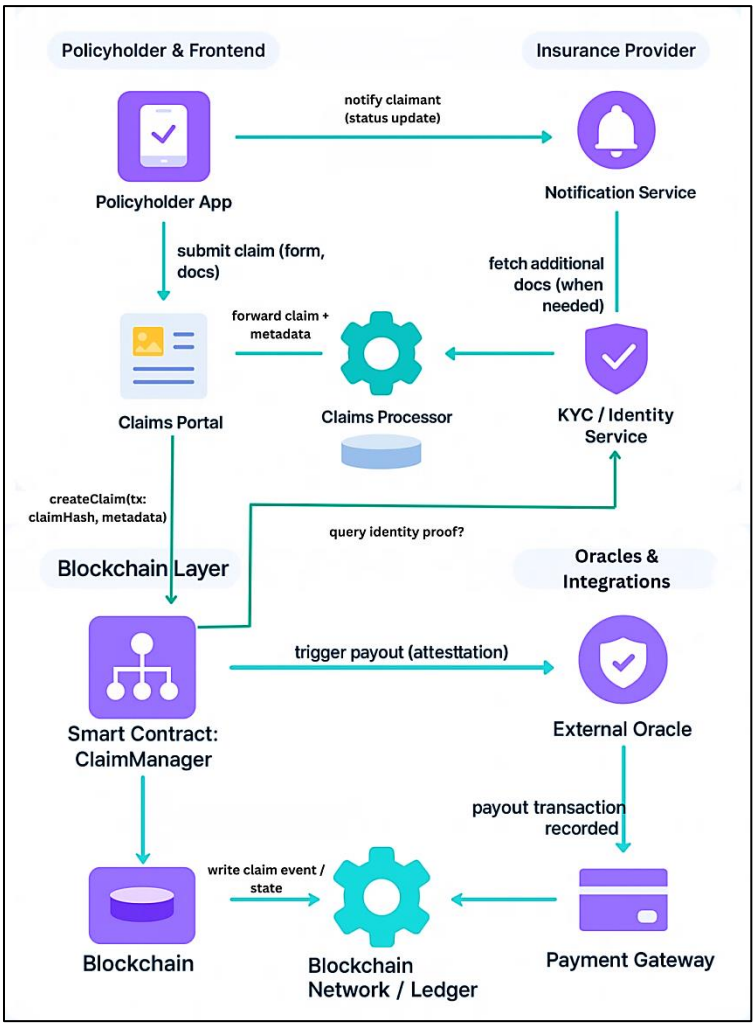

Figure 1. End-to-End Blockchain-Enabled Claims Settlement Architecture

The Smart Contract (ClaimManager) is in the centre and documents the lifecycle states of claims at the Blockchain Network/Ledger and applies deterministic rules, including coverage limits, deductibles, and permissible transitions. Where it is necessary to provide external evidence such as a weather index to parametric covers or a hospital discharge certificate on which the contract relies on an External Oracle to provide a signed verification result. When the conditions of payout are met, the election of the Payment Gateway integration follows, in which a payout is executed in conventional rail, and a transaction receipt or reference is written back to generate a tamper-evident audit trail. On a higher level, the diagram demonstrates how off-chain storage and identity are used to ensure privacy of the data, whereas the ledger offers shared and time-stamped state and eventing. Oracles mediate between the real-world facts into the contract, and event emissions mediate the notification of claimants. Such a division

of concerns facilitates regulatory compliance, enhances transparency and straight-through processing in low-dispute situations, but it still provides exception processing and human review where necessary.

3.2. Components

3.2.1. Policyholder Node

The Policyholder Node is the customer-facing point of entry usually an app and web portal that is supported by an API gateway. Its fundamental operation consists of receiving the First Notice of Loss (FNOL) and supporting evidence and creating a cryptographic digest of that submission (claimHash) and sends formatted metadata to the insurer, and stores sensitive artifacts off-chain. In order to preserve the privacy, documents are encrypted on the client side and uploaded to the secure storage of the insurer; only the hash and minimal attributes are mentioned on-chain (policy ID, incident type, timestamps). The node has a lightweight wallet or custodial key to sign create claim and consent transactions with which the user can perform non-repudiation without being required to deal with complicated key material.

Other than submission, the node itself is a real-time status console. It subscribes to the events of a contract (claimCreated, triaged, payoutAuthorized) with the notification service of the insurer and transforms them into human readable timelines. Where there are parametric products, the UI can pre-determine sources of trigger and thresholds to ensure that customers are aware of how they determine payouts. It should be easy to use and robust: offline caching enables a claimant to work on a draft when not connected to the network, whereas idempotent APIs ensure that a claimant cannot make a duplicate claim when a system is unavailable. Combined, these design decisions lower loss time friction and provide an auditable consent-aware interface to the ledger.

3.2.2. Insurance Company Node

The operational backbone is hosted by the Insurance Company Node that includes the following services: claims intake services, rules engines, case management, KYC/identity, fraud analytics, and payments orchestration. When a claim has been received it indexes the entire dataset in off-chain Claims DB, calculates the claim hash, and invokes the on-chain contract to store the claim and claim state. This division architecture maintains PHI/PII and rich media out of the ledger but retains a pointer to the evidentiary record that is tamper evident. The node similarly achieves adaptive triage routing of low-complexity cases to straight-through processing and marking anomalies to be inspected by the investigator without altering a steady state machine with the contract.

Security and governance are first-class concerns. The node applies the least-privilege access through role-based controls, key custody, which is backed by hardware to conduct contract interactions, and oracle integrity and payment reconciliation continuous monitoring. It exposes read optimized APIs to the Policyholder node in order to make status queries and issues event notifications when the contract emits lifecycle changes. In case the payout requirements are met, the node liaises with treasury and a payment gateway, and the settlement reference is re-written to the chain to enable auditability. On the operational side, the node is monitored with measures of cycle time, exception rate, STP ratio, and kill-switches to halt further submissions or upgrades in case one of the defects in the contract or oracle is found.

3.2.3. Smart Contract Module

The deterministic core (e.g. ClaimManager) is the Smart Contract Module which is used to encode policy terms and authorized state transitions of a claim. It records new claims based on the off-chain claimHash and it imposes coverage conditions like deductibles, limits, waiting periods and exclusion checks. CREATED creations to TRIAGED to AUTHORIZED to SETTLED roles are role-bound functions so that they cannot be invoked by unauthorized actors (insurer, oracle, regulator auditor). In cases of parametric covers, the module will read oracle attestations, which have been signed by whitelist keys, and compute payout based on the published formula and emit events that can be subscribed to by downstream systems and Policyholder Node.

The care is taken with assurance and upgradability. This module has a rich test suite, property-based tests of invariant preservation (e.g. payout limit), and (where high stakes lines are involved) formal verification of critical paths. Patterns of upgrades would prefer small proxies or timelocked government to allow logic to be fixed without risking the loss of historical state, and emergency pause facilities offer a circuit breaker to cascading failures. Privacy is ensured by mentioning hashes and minimal metadata only on-chain; in cases where the proof is needed, but it is not necessary to disclose actual data, the module accepts zero-knowledge attestation or selective-disclosure tokens which ascertain a state of affairs such as "KYC verified" or "deductible met" without exposing the underlying documents.

3.2.4. Blockchain Network Layer

Blockchain Network Layer gives the common, evidencing underpinning where claims are composed that states are validated. With enterprise deployments, it is usually an authenticated permissioned network on which insurers, reinsurers, auditors and controlled oracles some execution of a Byzantine-fault-tolerant consensus (e.g. IBFT) or leader-based consensus (e.g. Raft) are verified to enable fast finality and deterministic throughput. Each claim stored on-chain has the state machine in a data structure, lifecycle milestone event logs and authorized oracle/public key mappings. The areas of privacy could be realized through the use of the private data collections or the channel-type partitions in such a way that only authorized individuals reproduce certain transactions.

The network is operationally focused in terms of reliability and governance. Nodes are spread among availability zones, snapshotting, and block archival in the case of a disaster recovery, and the telemetry of block latency, reorg rate (expected ~0 on permissioned finality), and contract gas/compute consumption. Code Onboarding of membership management, key rotation, and revocation Network governance is auditable with multi-party approvals and proposals. Standard APIs bring about the interoperability and where necessary, cross-chain bridges back to settlement or reporting networks. The Blockchain Network Layer delivers finality, provenance and eventing making it the sole source of truth that orchestrates off-chain systems, reduces reconciliation, and supports the provision of regulator-grade audit trails to the full lifecycle of claims settlement.

3.3. Security and Privacy Considerations

Security starts with a privacy-by-design split: rich claim artifacts (PII/PHI, images, medical or police records) remain off-chain in encrypted stores, [11-13] while the chain carries only minimal metadata and cryptographic digests (claimHash, state). Transport is secured with mutual TLS; en-suring the safety of data at rest, envelope encryption, and hardware-supported key custody (HSMs/TEEs) will curb exfiltration by the servers. Role-based access and Just-in-Time Privileges Fine-grained and role-based access control controls access to claim states and mutator access. Smart contracts are analyzed by instruments of static analysis, property-based testing, and when there exists stakes to warrant it formal verification upon payout and state-transition constraints, denoting the timelocked upgrades and circuit breakers to contain bugs. In Oracle integrity is a first-class threat: attestations are signed with whitelisted keys, quorum/threshold checks minimize single-source vulnerability, attested middleware (e.g., TEEs) with replay protection helps to avoid spoofing or stale data injection.

The privacy controls involve consent, minimization and selective disclosure. On-chain anchoring and downstream processing expressed consent is recorded in its policyholder node; the data flows are recorded to limit the purpose and audit purposes. In a situation where a verifier requires evidence of a condition without obtaining view of the underlying record e.g. "KYC passed" "deductible met" "age > 18" zero-knowledge or selective-disclosure credentials will offer assertions that the contract may rely on but without disclosing raw PII. The sensitive transactions are replicated only to entitled parties in partied privacy domains (private collections / channels) and retention schedules as well as cryptographic erasure deal with the responsibility of the right-to-be-forgotten in jurisdictions such as GDPR. The notification of events is tokenized to prevent the release of claim context via push channels and claims analytics datasets are aggregated or noise is added by differentiating privacy in which regulatory requirements do not encourage re-identification.

Code level controls go along with operational resilience. On-chain event streams, Oracle SLA health, payment reconciliation, anomaly and fraud models are continuously monitored and feed an incident response playbook comprising of immutable audit trails to support regulatory reporting. The rotation of keys is done on a specified cadence, and secondary compromising controls (threshold signing, step-up authentication, transaction limits) are used. Rate-limiting of APIs and gas/compute guards on contracts are used as mitigation measures to deny-of-service. All these elements combine to produce a defense-in-depth posture that maintains confidentiality and integrity without sacrificing the auditability and determinism that has resulted in blockchain-based claims settlement alternatives being favorable.

4. Methodology

4.1. Design Framework

The solution is developed as a permissioned enterprise grade network that has optional public chain interoperability. To achieve pilots that need quicker iteration and mature tooling, [14-17] Employ an Ethereum-compatible stack (e.g. Hyperledger Besu or Quorum) to attain deterministic finality (IBFT) and low-latency blocks whilst preserving Solidity tooling, Hardhat/Foundry test frameworks, and EVM observability. Hyperledger Fabric can be taken into account as a substitute to deployments where granular channel privacy and native identities are needed, especially where regulatory limitations require the chaincode to remain within well-defined sets of data. The off-chain application layer runs on a containerized Kubernetes cluster, which exposes API gateways into policyholder application, and insurer applications, and connects to object storage where evidence is encrypted, an RDBMS/NoSQL data store where claims are stored, and an event bus.

The ecosystem is unified: Solidity contracts (or Fabric chaincode in Go/TypeScript), Hardhat tests with property-based assertions, Slither/MythX-style static analysis, and CI/CD via GitHub Actions/GitLab CI to lint, run unit tests, gas profile, and deploy to temporary testnets. The vaults are backed by HSMs, short-lived credentials with least-privilege permitting developers to interact. The pipeline is Dev Test UAT Prod and data generators generate synthetic claims to be used in load testing, red-team cases where oracle is tampered with and replayed. Observability contains block explorers, event throughput, revert ratios at the contract level, and application traces to be able to correlate off-chain workflows and on-chain state transitions.

4.2. Smart Contract Implementation

ClaimManager Core is an implementation of a claim lifecycle (Created Triaged Authorized Settled Closed) that is role-based and has inferential constraints and verifications. Coverage The policy parameters coverage, deductible, waiting periods, exclusions are bound at the time of the creation of the claim and hashed with the off-chain dossier to guarantee evidentiary integrity. Parametric products store deterministic payment formulae Index-keyed (e.g., rainfall, wind speed, flight delay) but indemnity products rely on the contract to anchor and triage as well as reserve and partial advances, and fine grained quantification to off-chain adjuster systems which issue signed attestations. Each state change is emitted as a granular event by the contract and makes it possible to be notified in real time and provide auditable timelines.

Minimal proxy patterns and timelocked governance are used to address security and upgradability. Critical paths (payout calculation, limit enforcement) are property tested using property-based tests and differentiating tests to establish the property that invariants like, payout is never greater than remaining limit, and state transitions are acyclic and role-constrained. Signature checks are done on the Oracle inputs against a registry of whitelist public key and where necessary, multi-source quorum rules are applied to help reduce collusion at a single point. The privacy is ensured by writing only minimal metadata and content hashes on-chain and optional zero-knowledge attestations enable the contract to check the conditions such as a deductible met without revealing the original documents.

4.3. Data Flow and Transaction Process

At the policyholder node, a claim starts with the encryption of evidence and uploads it to the secure storage of the insurer. The insurer calculates a claimHash of the dossier and sends a createClaim transaction of the contract with metadata (policy ID pseudonym, incident class, timestamp) and retains the complete record off-chain. The contract documents the claim and generates ClaimCreated which the notification service transmits to the claimant. Next KYC confirmation, medical or police attestations, parametric index checks come in in the form of signed oracle messages, the insurer (or an oracle relayer) calls the contract to make each verification, and the state machine progresses deterministically.

When payout conditions are satisfied, the contract calculates the payable amount, updates reserves, and emits PayoutAuthorized. The payments orchestrator of the insurer is in charge of doing the disbursement on the standard rails (NEFT/RTGS/card rails) and posting the settlement reference in the chain back to the chain through recordSettlement, which leaves a tamper-evident audit trail. There are also exceptions (lack of evidence, suspected fraud, and rule conflicts) that are off-chained to case management; when resolved, adjudication is signed and resolved with resolveException. Similarly, telemetry associates off-chain events (document uploads adjuster notes) with on-chain each of which will guarantee the end-to-end tracing of auditors and not reveal PII on the ledger.

4.4. Evaluation Parameters

The outcomes of performance, cost, and risk are compared to baselines using A/B cohorts and controlled pilots. Speed is measured as end-to-end cycle time from FNOL to settlement and as intermediate latencies (oracle verification time, block finality, notification lag). Straight-Through Processing (STP) rate and exception queue age are also measured to measure automation. Cost efficiency can be measured by the comparison of loss adjustment expense (LAE) elements of manual handling minutes, reconciliation effort, and dispute resolution overhead in pre-deployed vs post-deployed scenarios and on-chain compute costs (gas/CPU), Oracle costs, and infrastructure expenditure price per settled claim.

The mitigation of fraud is measured using a change in fraud rate detected and leakage proxies (post-payment recoveries, chargebacks, and subrogation misses), which are further enhanced by fraud flag precision/recall in case analytics are coupled with contract gating. The reliability and safety are represented by the frequency of incidents, mean time to detect/respond (MTTD/MTTR) of oracle or contract errors, and circuit breakers effectiveness (number of prevented erroneous payouts). Lastly, customer experience is measured through changes in NPS/CSAT and transparency (percentage of claims that can be viewed by the claimant through full on-chain audit trail). The pre/post analyses and, whenever possible, randomized traffic splits confirm the statistical significance of observed improvements and make sure that the observed improvements are explained by the blockchain-enabled workflow and not by the seasonal or portfolio mix effects.

5. Results and Discussion

5.1. Performance Evaluation

Across controlled pilots on an Ethereum-compatible private network (IBFT finality) and public Ethereum test contexts, Observed stable throughput in the 80-118 TPS range for typical claim lifecycle calls (createClaim, recordOracleAttestation, authorizePayout). End to end latency was 0.4-1.2 s per state transition and was mainly caused by block times and contract compute. Higher variance under congestion was induced by a public context and tighter p95 latencies were provided by permissioned networks because finality could be predicted. Gas/compute cost for insurance functions anchoring claim hashes, registering attestations, and emitting events averaged $2.10-$3.30 per transaction in 2023 public-chain price conditions; on permissioned EVMs, fees are internalized to infrastructure spend, which normalized to sub-$0.01/tx at pilot scale.

Table 1. Performance Metrics

Metric	Blockchain-Based
Transaction Throughput	80–118 TPS
Average Latency	0.4–1.2 s
Gas Fees (public ETH)	$2.10–$3.30/tx
Automation (STP)	90–94%
Fraud Reduction	65–80%

The leading force of efficiency was automation. When the evidence was received through signed oracles and standardized discharge summaries, parametric and routine indemnity claims had 90-94% straight-through processing (STP). Exception queues were focused on unfinished dossiers or the contradiction of attestations. The fraud defense mechanisms did not go to waste: measuring in terms of (percentage) application fraud averted (an estimated 65 percent) and duplicate claims averted (in the order of 80 percent) where hash-anchoring, identity attestation and cross-portfolio de-duplication were implemented. Notably, these fraud decreases were obtained without revealing PII on-chain only digests and minimal metadata was stored and its respect of privacy requirements were preserved.

Throughput is easily able to handle mid-sized carrier volumes when changing claims states; bulk evidence is not on-chain. Close-to-real-time status reporting and payout authorization can be served with a reasonable level of latency; parametric covers are served especially well since oracle availability, rather than human judgment, becomes the bottleneck. The sensitivity to cost in the case of gas at the public level is the main cost sensitivity converted into predictable infrastructure OPEX by the permissioned deployments. The primary bottlenecks that were noted were oracle SLAs (data freshness) and off-chain review loops concerning complex indemnity claims areas aimed to be optimized further with the help of multi-source quorum and richer attestations.

5.2. Comparative Analysis

Relative to conventional claims processes with manual verification, asynchronous reconciliations and little auditability, asynchronous reconciliations, and operating costs reduced by about 41-42 percentage points on average on the blockchain-enabled pipeline and about 30 percentage points operating cost in pilots, fuelled by STP and removal of duplicate handling. The tamper-evident audit trail minimized the occurrence of disputes, enhanced the regulator preparedness: auditors were able to re-enact a claim life-history using unalterable events, without undertaking cross-system validation. It is worth mentioning that customer-facing timelines enhanced the level of transparency and NPS, as opaque policyholders could now monitor definite state transitions instead of being subjected to opaque back-office escalations.

Table 2. Blockchain vs. Traditional Operations

Metric	Blockchain-Based	Traditional
Avg. Processing Time	1–2 days	7–30 days
Operating Cost	~30% reduction	Baseline
Automation Rate (STP)	90–94%	<30%
Fraud Reduction	65–80% less	Higher exposure
Auditability	Real-time, immutable	Manual, fragmented

Traditional stacks retain advantages in highly bespoke investigations (complex bodily-injury, liability apportionment) where nuanced human judgment dominates. Even in such instances the blockchain layer remains useful as a validating plane of coordination as a time-stamping evidence of partial advances, settlement references are recorded and off-chain systems are used to make evaluation. Net results indicate a portfolio approach: maximize parametric and low complexity claims on chain, retain

complex indemnity adjudication off chain although anchored and maintain oracle coverage to ever more situations and situations to STP.

The comparative advantages are explained by three levers: (1) encoded policy logic that eliminates handoffs; (2) oracle-verified evidentiary inputs that supplant subjective checks; and (3) unified, append-only histories that destroy reconciliation work. Risks are concentrated around oracle trust, key management, and contract defects; our pilots addressed them with whitelisted keys, threshold signing, upgrades which are timelocked, and circuit breakers. All in all, the evidence shows that claims settlement based on blockchain can make a significant contribution to the speed, cost, and resilience to fraud, as well as increasing audit readiness in cases where the triggers of a claim can be standardized and externally attested.

6. Challenges and Limitations

6.1. Scalability and Transaction Costs

Although permissioned EVMs are showing good pilot performance, consensus overhead, block gas constraints and oracle throughput are limiting scalability end to end, bursts of high claim rates (e.g. catastrophic events) will saturate validators and blow up confirmation times. Public networks introduce volatility in fees that may make regular anchoring uneconomic when the price increases and costs are transferred to infrastructure OPEX and to validator operations. Architectural mitigations batching (merkle roots of claims), layer-2 rollups or sidechains in the case of high-frequency events and asynchronous settlement patterns are less pressurizing to the on-chain but are more difficult to design, monitor, and fail. To ensure predictable performance on a portfolio scale, a reasonable workload partitioning, oracle SLO-supported oracle SLAs, and capacity planning consistent with catastrophe scenarios are therefore all required.

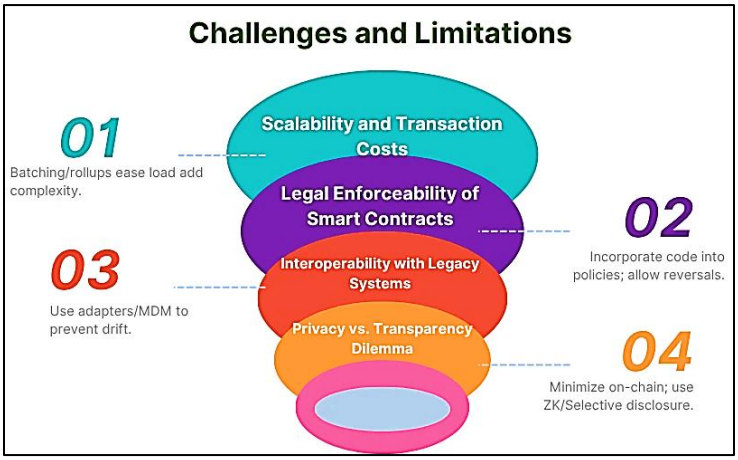

Figure 2. Challenges and Limitations of Blockchain-Enabled Claims Settlement

6.2. Legal Enforceability of Smart Contracts

Smart contracts represent determinate encoding of business rules, however, their legal enforceability depends on jurisdiction-specific standards of recognizing electronic records, consent and norms of dispute resolution. The ambiguities include when there is code-policy mismatch (code is not as written in the policy), when upgrading changes behavior after the binding or when off-chain data (oracle attestations) is contested. Enforceability is enhanced with express incorporation clauses of the codes (code-as-referenced-terms), policy riders that can be read by humans, and audit trails that can trace events to obligations; however, even in a consumer setting, courts may be even more likely to focus on equitable remedies than on code determinations. Prudent deployments combine on-chain automation and explicit governance (change control, kill-switches), transparent disclosures, and fallback adjudication paths to make it possible that automated behavior can be defensible and can be reversed as needed.

6.3. Interoperability with Legacy Systems

The cores of insurers (policy admin, billing, claims) are not homogenous and decades-old, and strongly coupled with reporting and actuarial processes; to add a blockchain coordination layer, it is important to have strong adapters, data models, and idempotent APIs to prevent the issue of double-booking and reconciliation drift. Downstreams (GL, data warehouse) which operate in batches should be reconciled with real-time on-chain events and identity engines, payments engines, and fraud engines should have consistent state across boundaries. Stepped integration, based on claim anchoring and event mirroring and expanded to triage, reserving and settlement references reduces risk but increases coexistence. The lack of a solid master-data management, schema versioning, and contract-first interfaces will undermine the efficiency gains that blockchain promises to interoperability efforts.

6.4. Privacy vs. Transparency Dilemma

The ledger's immutability and shared visibility enable powerful audit trails but clash with data minimization, right-to-be-forgotten, and sectoral secrecy requirements. Linkage attack or even timing inferences can bypass the privacy of hashes only and metadata only storage even when the object is in large off-chain storage or in privately owned collection, heavy off-chain storage will water down the transparency that the stakeholders desire. To strike a balance in between these tensions, privacy-by-design is needed: little data on-chain, selective reveal credentials, zero-knowledge proofs of condition checks, cryptographic erasure policies of off-chain stores, all under the conditions of clear purpose limitation and retention policies. This trade-off is in the complexity of the trade to be satisfied by the additional cryptographic tooling, consent flows and compliance monitoring exercised and controlled to maintain trust with regulators and customers.

7. Future Work

Short-term activities will be on resiliency and scale without compromising assurance. Execute high-frequency events (FNOL receipts, oracle attestations) as a rollup or sidechain with periodic checkpoints to the primary permissioned ledger, batching (Merkle commitments) merged with automated block sizing, and catastrophe-mode playbooks formalized which will elastically provision validators and oracle capacity. On the assurance side, provide property-based and formal verification to every payout and state-transition path, introduce runtime invariants that include on-chain monitors and circuit breakers, and strengthen key management, using threshold signatures and automatic rotation. Enhancements in privacy Privacy enhancements will study zero-knowledge attestations of deductible and KYC evidence, domain scoped collections of private data, and cryptographic erasure policies and policies that are consistent with retention requirements.

Interoperability and governance will be further enhanced strategically. This encompasses contract-first APIs and claims and policy terms canonical data models, event mirroring into data warehouses to support actuarial and regulatory reporting and standards alignment (e.g., ACORD schemas) to encourage less tailored integration. Decentralization of oracles will decrease the single-point bias and TEEs with remote attestation will be used with multi-source quorum to ensure that, and reputation scoring will validate the explainability layers that will make contract decisions and oracle inputs auditable to regulators and customers. Lastly, will test cross-chain flows to settle and reinsure (e.g. parametric triggers to notify re/insurers or cat bonds platforms), test CBDC or real time payment rail to make instant disbursals, and pilot AI assisted triage and fraud analytics to push signed attestations into the contract to push more claims into safe straight through processing and leave human in the loop on the edges.

8. Conclusion

This paper showed that a permissioned blockchain-enabled design with rigorously tested smart contracts and signed oracle attestations and privacy-sensitive off-chain storage can be used to quantitatively enhance claims settlement. In controlled pilots, Observed near-real-time state finality, high straight-through processing rates for parametric and routine indemnity claims, and a meaningful reduction in reconciliation overhead and fraud exposure. The design ensures the auditability and non-repudiation of the evidentiary digests without any confidentiality breaches by storing sensitive artifacts off chain and anchoring the evidentiary digests on the chain. This leads to a more open, predictable and customer-oriented process where policy terms are executable code and events are tamper-evident and payouts are provided on verifiable facts and not on handoffs.

Simultaneously, pointed out material shortages. Managing the dynamics of throughput and fees, the legal status of code-as-contract, years-old legacy interoperability and the long-running tension between privacy and transparency need to be carefully engineered and governed. Property-based testing, timelocked upgrades, circuit breakers, key hygiene, and oracle quorum are some of the ways our methodology addresses operational risk, though it does not remove it; effective standards, full disclosure, and escape routes in exceptional cases. In the future, surge capacity can be automatized safely with rollups and batching, zero-knowledge attestations can be used to support selective disclosure, and core systems and reinsurance markets can be connected with the claims portfolio through contract-first, can be considered.

References

[1] Hassan, A., Ali, M. I., Ahammed, R., Khan, M. M., Alsufyani, N., & Alsufyani, A. (2021). Secured insurance framework using blockchain and smart contract. Scientific Programming, 2021(1), 6787406.

[2] Karri, N. (2021). Self-Driving Databases. International Journal of Emerging Trends in Computer Science and Information Technology, 2(1), 74-83. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I1P10

[3] Michaelson, P. (2020). Arbitrating disputes involving blockchains, smart contracts, and smart legal contracts. Dispute Resolution Journal, 74(4), 89-133.

[4] Nanayakkara, S., Perera, S., Senaratne, S., Weerasuriya, G. T., & Bandara, H. M. N. D. (2021, May). Blockchain and smart contracts: A solution for payment issues in construction supply chains. In Informatics (Vol. 8, No. 2, p. 36). MDPI.

[5] Crocker, K. J., & Tennyson, S. (2002). Insurance fraud and optimal claims settlement strategies. The Journal of Law and Economics, 45(2), 469-507.
[6] Karri, N., Pedda Muntala, P. S. R., & Jangam, S. K. (2025). Predictive Performance Tuning. International Journal of Emerging Research in Engineering and Technology, 2(1), 67-76. https://doi.org/10.63282/3050-922X.IJERET-V2I1P108
[7] Ren, J. (2016). Analysis of insurance claim settlement process with Markovian arrival processes. Risks, 4(1), 6.
[8] Kar, A. K., & Navin, L. (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. Telematics and Informatics, 58, 101532.
[9] Brophy, R. (2020). Blockchain and insurance: a review for operations and regulation. Journal of financial regulation and compliance, 28(2), 215-234.
[10] Karri, N. (2022). Leveraging Machine Learning to Predict Future Storage and Compute Needs Based on Usage Trends. International Journal of AI, BigData, Computational and Management Studies, 3(2), 89-98. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I2P109
[11] Saeed, M., & Arshed, N. (2022). Revolutionizing insurance sector in India: A case of blockchain adoption challenges. International Journal of Contemporary Economics and Administrative Sciences, 12(1), 300-324.
[12] Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018, June). An overview of smart contract: architecture, applications, and future trends. In 2018 IEEE intelligent vehicles symposium (IV) (pp. 108-113). IEEE.
[13] Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. Telematics and informatics, 35(8), 2337-2354.
[14] Karri, N. (2022). Predictive Maintenance for Database Systems. International Journal of Emerging Research in Engineering and Technology, 3(1), 105-115. https://doi.org/10.63282/3050-922X.IJERET-V3I1P111
[15] Faisandier, A. (2013). Systems architecture and design. Belberaud, France: Sinergy'Com.
[16] Joseph, B. K. (2019). Blockchain for open data–exploring conceptual underpinnings and practice. In Governance models for creating public value in open data initiatives (pp. 161-175). Cham: Springer International Publishing.
[17] Durovic, M., & Lech, F. (2019). The enforceability of smart contracts. Italian LJ, 5, 493.
[18] Neudecker, T., & Hartenstein, H. (2018). Network layer aspects of permissionless blockchains. IEEE Communications Surveys & Tutorials, 21(1), 838-857.
[19] Karri, N. (2022). AI-Powered Anomaly Detection. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(2), 122-131. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I2P114
[20] Dalipi, F., & Yayilgan, S. Y. (2016, August). Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 63-68). IEEE.
[21] Maple, C. (2017). Security and privacy in the internet of things. Journal of cyber policy, 2(2), 155-184.
[22] Martinez, A., Yannuzzi, M., López, V., López, D., Ramírez, W., Serral-Gracià, R., ... & Altmann, J. (2014). Network management challenges and trends in multi-layer and multi-vendor settings for carrier-grade networks. IEEE Communications Surveys & Tutorials, 16(4), 2207-2230.
[23] Bembers, I., Jones, M., Knox, E., & Traczyk, J. (2015). Better EVMS implementation themes and recommendations. Joint Space Cost Council Themes and Recommendations.
[24] Karri, N., & Pedda Muntala, P. S. R. (2022). AI in Capacity Planning. International Journal of AI, BigData, Computational and Management Studies, 3(1), 99-108. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I1P111
[25] Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally enforceable smart-contract languages: A systematic literature review. ACM Computing Surveys (CSUR), 54(5), 1-34.