IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Oracle For Digital Transformation In Financial Sector

[1]Urvi Satish Kolawala, [2]Veena Jokhakar

[1]Teaching Assistant, [2]Assistant Professor

[1]Department of ICT,

[1]Veer Narmad Sount Gujarat University, Surat, India

Abstract: The financial sector faces major challenges such as inefficiencies in claims processing, lack of transparency, high operational costs, and reliance on intermediaries. This research explores blockchain technology as a solution to create a decentralized, transparent, and secure claims management framework. By integrating smart contracts and cryptographic techniques, the proposed IP-NS-FS-BLKCHN model aims to enhance trust, efficiency, and compliance, benefiting both customers and organizations in the insurance industry.

Keywords - Blockchain, Smart Contract, Consensus, Distributed Application, Inter Planetary File System, Internet Planetary Network Systems, Oracle

I. INTRODUCTION

Historically, the functioning of Financial Services relies on the trust established between service providers and their customers, a process that is carried out manually. This manual handling can lead to both unintended and intentional errors in processing requests[1]. Such a method of operation exposes it to numerous challenges, including mismanagement and misunderstandings, which can result in financial losses or detrimental effects on users' health. Individuals engage in daily transactions involving vehicles, which are monitored by transportation authorities as part of fleet management to log aspects like location, timing, or load weight. However, managing these transactions becomes challenging when dealing with large volumes of data. For instance, in the realm of trades concerning vehicles during everyday operations, transportation authorities also oversee vehicle transactions as a part of fleet management. Nevertheless, tracking these transactions is a challenge, as highlighted by T. A. Syed et al.[5].

Financial service providers are currently navigating significant pressure from several directions, including cost increases, heightened customer expectations, and technological disruption. The industry landscape is fundamentally changing as smaller competitors harness technologies like AI, IoT, and blockchain to deliver innovative customer experiences. While these innovations could eventually pose a significant disruptive threat to traditional firms, established insurers still benefit from powerful competitive advantages. These advantages stem from their long-standing customer relationships, deep-seated expertise, and a rich trove of data gathered from operations, partners, and the broader market.

Driven by the need to boost efficiency, increase transparency, and improve customer experience, the insurance industry has been embracing a wide range of new technologies as part of its digital transformation.

To protect against financial or asset loss, the modern era demands fundamental changes to the working, validation, and operational methods of financial services. These changes must ensure identity, security, and validity are maintained throughout the entire process, right up to maturity, redemption, or claim settlement.

The insurance sector, in particular, requires a transformative solution designed to simultaneously increase operational efficiency, foster innovation, and build stakeholder trust. Enhanced claim processing transparency and speed are critical; they will help insurers reduce delays, lower costs, and curb malpractice. By streamlining operations and removing unnecessary intermediaries, faster settlements and a much improved experience will be delivered to customers and partners.

Blockchain technology accelerates claims and settlements in the insurance sector, while simultaneously guaranteeing transparency and fairness. This innovation combats inefficiencies by utilizing a decentralized structure to enhance fraud detection, simplify underwriting, and enable smooth client onboarding. Integrating blockchain components allows businesses to grow their networks, establish trust, and secure a competitive advantage. The result is a system with superior operational efficiency, greater customer satisfaction, and refined risk assessments, positioning the industry for continuous advancement and growth.

The structure of the paper is straightforward: Section 4 covers related work. Section 5 explains the technologies used. We detail the proposed framework for insurance service blockchain DApps in Section 6. Section 7 provides the conclusion.

II. Related Work

In [2], Castro et al. explore Hybrid consensus models designed to overcome the limitations of individual protocols. They provide the example of a PoW/PoS hybrid that combines the security of PoW with the energy efficiency of PoS to achieve better balance. The authors also discuss Practical Byzantine Fault Tolerance (PBFT), noting its robust security and reliability for permissioned networks, while acknowledging its drawbacks concerning scalability and high resource consumption in larger environments. A key limitation they identify for all hybrid models is the increase in operational complexity and the need to manage potential security trade-offs.

According to Zhang et al. [3], sharding implementations are complicated by problems with inter-shard communication and a heightened risk of security breaches. Furthermore, they highlight that off-chain solutions are limited by their potential failure to guarantee finality and the fundamental reliance on trust between participants.

Chen et al. [4] explore Decentralized Finance (DeFi) and Smart Contracts, noting that DeFi platforms leverage these contracts to deliver intermediary-free financial services like lending, borrowing, and trading. The primary benefits of these platforms include lower fees, enhanced transparency, and global accessibility. However, the authors caution that the inherent complexity of smart contracts introduces significant risks, specifically security vulnerabilities and scalability limitations, which become particularly evident during high-volume transaction periods. They specifically mention that DeFi on Ethereum struggles with scalability, resulting in high transaction fees, and that smart contracts are susceptible to bugs and security exploits, which can lead to substantial financial losses.

T. A. Syed [5] introduces a permissioned, Hyperledger Fabric-based blockchain system to track the full vehicle life cycle (manufacture through disposal, including insurance and leasing) with goals of openness, security, and trust. The framework integrates IoT devices for monitoring and uses RAFT consensus and smart contracts (chaincode) for automated, fault-tolerant operations. It includes a machine learning module for used car price prediction. A Saudi Arabia case study highlights its practical application and regulatory integration. Performance evaluation confirms its high scalability, security, and efficiency, ensuring tamper-proof records and fraud prevention for multi-stakeholder transactions worldwide.

The work by Ankit Kumar et al. [6] offers a comprehensive analysis of blockchain consensus algorithms with respect to transaction validation, security, and the challenge of scalability. The study covers a wide spectrum of mechanisms, including PoW, PoS, PBFT, Bitcoin-NG, ByzCoin, and WBFT. The authors detail the core scalability issues—such as network latency and block size limits—and categorize proposed solutions into on-chain, off-chain, and improved consensus protocols. A key feature is the comparative analysis of these solutions' throughput, fault tolerance, and node scalability. The paper illustrates their relevance across various applications (e.g., healthcare, IoT, and supply chains), emphasizing that scalability improvements are essential for the widespread adoption of blockchain technology.

Recognizing that traditional Health Insurance Claim (HIC) systems suffer from fraud, inefficient manual checks, and centralized security weaknesses, K. Kapadiya [7] introduces a combined Blockchain and AI system for enhanced transparency and fraud detection in healthcare insurance. This solution uses Blockchain to ensure tamper-proof records and employs AI/ML models (supervised, unsupervised, and hybrid) to flag fraudulent claims. Smart contracts automate claim verification, leading to increased efficiency and reduced human involvement. A novel aspect is the proposed use of wearable IoT devices for real-time validation of medical events. Kapadiya further examines the security landscape, addressing issues like data privacy and cyber threats. The paper asserts that to achieve effective fraud detection, industry focus must be on scalability, standardization, and training skilled professionals. Ultimately, the AI-blockchain framework offers a scalable, secure solution that builds trust and automation in the industry.

In [8], a systematic literature review is conducted on blockchain applications in healthcare supply chains, underscoring the technology's contribution to efficiency, security, and transparency. The review covers 124 research papers, identifying major applications such as managing EHRs, tracking drugs, preventing insurance fraud, and facilitating remote patient monitoring. The use of blockchain helps to reduce fake drugs and guarantees safe, decentralized data exchange. Conversely, the authors detail significant difficulties, including steep implementation costs, privacy issues, and regulatory hurdles. The study's examination of blockchain's integration with AI, IoT, and smart contracts provides valuable insights for policymakers and stakeholders seeking to optimize healthcare supply chain management.

The paper [9] examines a blockchain-based solution for safe and transparent prescription health insurance claims. Implemented on a private Ethereum blockchain with smart contracts, the system automates registration and claim approval to reduce fraud and inefficiencies. IPFS off-chain storage ensures data security, and DApps improve access. By creating a tamper-proof network connecting insurers, pharmacies, and medical providers, the system enhances trust, automation, and transparency. Security analysis validates improved privacy, fraud prevention, and scalability. This decentralized framework simplifies claim processing, guaranteeing accuracy and cost savings.

The paper “A Study of Blockchain Oracles”[13] explores blockchain-based solutions that enable smart contracts to securely access real-world data. Since smart contracts cannot directly retrieve off-chain information, the study presents oracles as trusted interfaces that fetch, verify, and deliver external data to blockchain networks. Implemented through various models—software, hardware, human, and decentralized designs—these oracles expand the functionality of blockchain applications across diverse sectors. By examining frameworks such as Chainlink and Provable, the paper highlights how decentralized oracles reduce single points of failure and enhance data reliability. Security analysis emphasizes that while oracles improve automation and connectivity between blockchain and the real world, careful trust management is essential to prevent compromised data and ensure integrity, transparency, and resilience within smart contract ecosystems.

Sin Kuang Lo et al.[14] in their paper *“Reliability Analysis for Blockchain Oracles”* propose a framework to evaluate the dependability of blockchain oracles using Fault Tree Analysis (FTA). By modeling and comparing oracle mechanisms across platforms such as Provable, ChainLink, TownCrier, Corda, Augur, Gnosis, and Microsoft Bletchley, the study identifies weak points and major error sources, including human, software, and server faults. Results show that decentralized oracles achieve higher reliability than centralized ones, while human-involved systems are more error-prone. The framework provides a structured method to assess and improve oracle reliability, ensuring greater security and stability in blockchain-based systems.

Bartholic et al.[15] in their paper *“A Taxonomy of Blockchain Oracles: The Trusted Off-Chain Computing Problem”* present a classification of oracle systems based on trust, data flow, and decentralization. The study analyzes how oracles connect smart contracts with real-world data while addressing reliability and security challenges. It concludes that achieving trustless and verifiable oracle designs is key to ensuring secure and scalable blockchain applications.

Shahinaz Kamal Ezzat, Yasmine N. M. Saleh, and Ayman A. Abdel-Hamid[16] in *“Blockchain Oracles: State-of-the-Art and Research Directions”* present a comprehensive survey and taxonomy of oracle systems as the principal off-chain technique for enabling smart contracts to access real-world data; they compare oracles to other interoperability approaches, review major market solutions (e.g., Chainlink, Provable, Town Crier, DOS), identify strengths and weaknesses (trust, security, scalability, cost, latency), and outline design

best-practices and open research directions—concluding that oracles are a promising middleware for blockchain interoperability but require stronger decentralization, verifiability, and performance/cost improvements to address remaining trust and reliability challenges.

While work has been done on various fields using blockchain, no study or implementation has yet fully leveraged the combined advantages of blockchain, IPNS, IPFS, and oracles to create a highly secure system with no human or third-party involvement.

III. TECHNOLOGIES

1. Blockchain

   The launch of the Bitcoin white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," by Satoshi Nakamoto on October 31, 2008, established the foundation for both Bitcoin and blockchain technology [10]. At its core, a blockchain is a distributed database or ledger that is shared across thousands of computers, or nodes, globally. This network maintains an ever-expanding, chronologically ordered list of records known as blocks. The very design of the blockchain network makes it incredibly difficult to tamper with the stored data. Because breaking the system would require simultaneously hacking millions of networked computers, it is virtually immune to even the most potent supercomputers. All information is secured using cryptography, which is essential for securely linking the continuously growing chain of blocks.

2. Smart Contract

   A smart contract is essentially a set of rules encoded as a computer program that operates on the blockchain [11]. These programs automatically execute when a party satisfies the predetermined terms and conditions of an agreement. The agreement's conditions are permanently stored on the blockchain, contained explicitly within the smart contract's lines of code. Crucially, smart contracts eliminate the need for intermediaries, enabling trustless and permissionless financial transactions between users. Using "IF-THEN" programming logic, smart contracts are designed to automatically transfer, save, and receive money based on whether the coded conditions are met.

3. Consensus

   Traditional financial organizations depend on central authorities for system maintenance and security. In contrast, distributed networks use consensus algorithms to agree on a value. In blockchain, these protocols are crucial for ensuring all participants agree on the contents of a new transaction block and acknowledge the current state of the ledger [6]. The complexity of reaching consensus in a decentralized system prompts the question of how to maintain security and reliably track every transaction. The functionality and security of the blockchain are maintained by a set of protocols, incentives, and processes that facilitate agreement among a network of nodes. This governance structure underpins the safety and transaction verification for cryptocurrencies like Bitcoin, Ethereum, and Cardano.

4. IPFS

   For data storage and sharing, the InterPlanetary File System (IPFS) serves as a decentralized system that integrates seamlessly with blockchain technology. IPFS provides a method for efficiently storing large files off-chain, with the files' integrity verified by storing their unique cryptographic hashes onto the immutable blockchain ledger.

5. IPNS

   The InterPlanetary Name System (IPNS) is a decentralized naming system that operates within the IPFS ecosystem. Its primary function is to enable users to associate human-readable names with the content that is stored on the InterPlanetary File System (IPFS). IPNS leverages Public Key Infrastructure (PKI) to manage these name associations.

6. ORACLE

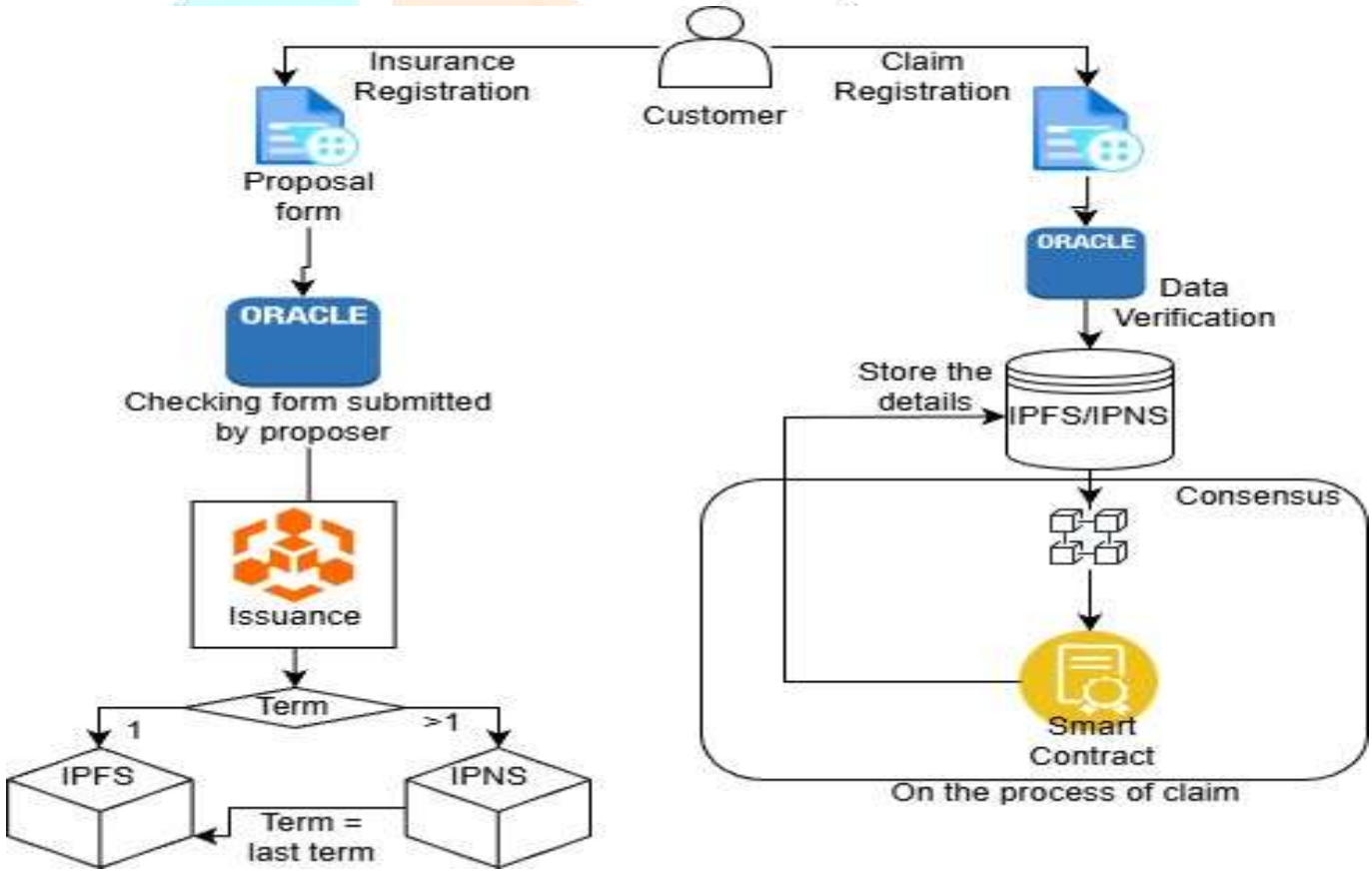
   While blockchain and smart contracts provide an immutable and trustworthy platform for agreement execution, they are inherently limited by their inability to access data from outside their native network—a challenge known as the "oracle problem." To resolve this, a blockchain oracle is employed, acting as a secure, decentralized bridge between the off-chain world (real-world data) and the on-chain environment

(the smart contract). In the context of the insurance industry, Oracles are critical because they are responsible for gathering, authenticating, and relaying real-world information—such as claim submissions or policy proposal details—to the smart contract. As an indispensable component of the IP-NS-FS-BLKCHN framework, the Oracle ensures that the smart contracts can operate effectively and reliably by feeding them verified, tamper-resistant data inputs, thereby enabling the automation of policy issuance and claim processing while maintaining a trustless environment.

IV. USE PROPOSED FRAMEWORK

This system models a decentralized insurance platform where blockchain technology ensures automation and trust. The lifecycle starts with the Insurance Registration process, where the customer submits a proposal that an Oracle verifies to bridge the real-world data onto the secure ledger. Once verified, the policy is issued, and its terms are stored in decentralized file systems, either IPFS or IPNS, ensuring immutability. When a claim is made, another Oracle confirms the veracity of the claim event. This validated claim data is then fed to a Smart Contract. The contract's code, which contains the automated policy logic, instantly processes the claim and executes the payment. The entire transaction is secured by the network's Consensus mechanism, creating an efficient, tamper-proof, and fully transparent path from policy issuance to claim settlement.

Fig.1 Oracle-Based Blockchain Consensus for Insurance Claims



Insurance Registration Process

The process begins when a Customer submits an Insurance Registration by filling out a Proposal form.

1. Oracle Verification (Proposal): The submitted Proposal form is sent to an Oracle, which performs a check on the form details provided by the proposer.
2. Issuance: If the form passes verification, the process moves to the Issuance stage.
3. Term Check: A decision point determines the insurance term:
4. If the Term = 1: The policy details are stored directly in IPFS (InterPlanetary File System).
5. If the Term > 1: The policy details are stored in IPNS (InterPlanetary Name System), and the Term is set to the last term (implying the policy has a changing or persistent name).

Claim Registration and Processing Process

The claims side of the process starts when the Customer initiates a Claim Registration.

1. Oracle Verification (Claim): The claim registration is sent to an Oracle for Data Verification.
2. Data Storage: The verified claim details are then stored in the IPFS/IPNS decentralized storage system.
3. Consensus and Smart Contract: The storage trigger initiates the blockchain's core process:
4. The claim details are used in the Consensus mechanism.
5. The validated details are then passed to the Smart Contract, which runs the logic for processing the claim ("On the process of claim").

V. CONCLUSION

As major entities like Financial Organizations and Governments become more interconnected, the need for secure, shared-resource communication between peers has driven the rise of Distributed Ledger Technology (DLT) and blockchain DApps globally. The future of networked communication, including industrial P2P systems, relies on blockchain's ability to establish an impenetrable digital ledger. This integrity is crucial for various applications, such as protecting intellectual property and improving data targeting. This paper's primary aim was to solve existing issues within the Insurance Industry by introducing the IP-NS-FS-BLKCHN framework. This solution innovatively combines IPFS, IPNS, and specialized consensus mechanisms for insurance issuance and claims. The framework ensures security, data sharing, immutability, and timely verification with updates to all stakeholders, eliminating delays in the process.

REFERENCES

[1] Amiya Karmakar, Pritam Ghosh, Partha Sarathi Banerjee, Debashis De,ChainSure: Agent free insurance system using blockchain for healthcare 4.0,Intelligent Systems with Applications,Volume17,2023,200177,ISSN26673053,https://doi.org/10.1016/j.iswa.2023.200177

[2] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI'99).

[3] Zhang, Y., et al. (2019). Sharding-based blockchain scalability solutions: A survey. International Journal of Computer Science & Information Technology, 11(2), 47-61.

[4] Chen, L., et al. (2020). Security and performance analysis of decentralized finance (DeFi) protocols. Journal of Blockchain Research, 11(2), 67-92.

[5] T. A. Syed, M. S. Siddique, A. Nadeem, A. Alzahrani, S. Jan and M. A. K. Khattak, "A Novel Blockchain-Based Framework for Vehicle Life Cycle Tracking: An End-to-End So- lution," in IEEE Access, vol. 8, pp. 111042-111063, 2020, doi: 10.1109/ACCESS.2020.3002170.

[6] Ankit Kumar Jain, Nishant Gupta, Brij B. Gupta,A survey on scalable consensus algorithms for blockchain technology,Cyber Security and Applications,Volume3,2025,100065,ISSN 2772-9184,https://doi.org/10.1016/j.csa.2024.100065.

[7] K. Kapadiya et al., "Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects," in IEEE Access, vol. 10, pp. 79606-79627, 2022, doi: 10.1109/ACCESS.2022.3194569.

[8] S. Dhingra, R. Raut, K. Naik and K. Muduli, "Blockchain Technology Applications in Healthcare Supply Chains—A Review," in IEEE Access, vol. 12, pp. 11230-11257, 2024, doi: 10.1109/ACCESS.2023.3348813.

[9] A. Alnuaimi, A. Alshehhi, K. Salah, R. Jayaraman, I. A. Omar and A. Battah, "Blockchain- Based Processing of Health Insurance Claims for Prescription Drugs," in IEEE Access, vol. 10, pp. 118093-118107, 2022, doi: 10.1109/ACCESS.2022.3219837.

[10] (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[11] Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. 10.1109/ICCCNT.2018.8494045.

[12] Zhai, Sheping & Yang, Yuanyuan & Li, Jing & Qiu, Cheng & Zhao, Jiangming. (2019). Research on the Application of Cryptography on the Blockchain. Journal of Physics: Con- ference Series. 1168. 032077. 10.1088/1742-6596/1168/3/032077.

[13] Beniiche, Abdeljalil. (2020). A Study of Blockchain Oracles. 10.48550/arXiv.2004.07140.

[14] Lo, Sin Kuang & Xu, Xiwei & Staples, Mark & Yao, Lina. (2020). Reliability analysis for blockchain oracles. Computers & Electrical Engineering. 83. 10.1016/j.compeleceng.2020.106582.

[15] M. Bartholic, A. Laszka, G. Yamamoto and E. W. Burger, "A Taxonomy of Blockchain Oracles: The Truth Depends on the Question," *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Shanghai, China, 2022, pp. 1-15, doi: 10.1109/ICBC54727.2022.9805555.

[16] Ezzat, Shahinaz & Nagi, Yasmine & Abdel-Hamid, Ayman. (2022). Blockchain Oracles: State-of-The-Art and Research Directions. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3184726.