Investigating Blockchain Consensus Models for Transparent and Efficient Insurance Systems

Urvi Satish Kolawala
Veer Narmad South Gujarat University
Surat, Gujarat, India

Veena Jokhakar
Veer Narmad South Gujarat University
Surat, Gujarat, India

ABSTRACT
Many industries are turning to blockchain as a potential new frontier, with benefits such as increased security and transparency and decentralisation. Through the analysis of consensus mechanisms, scalability, and sector-specific implementation issues related to blockchain development, this paper presents insights from 33 studies. Despite the operational complexity, hybrid consensus models like PoW/PoS and PBFT remain useful for balancing security as well as efficiency, according to key findings. It explores scaling solutions, including sharding and off-chain approaches, as well as their tradeoffs in cross-shard communication and trust.

Keywords
Blockchain, consensus mechanisms, scalability, smart contracts, decentralized applications, security, interoperability.

1. INTRODUCTION
A significant change is required in the modern period in the form of "digital transformation".

Digital transformation in financial services is using technology to optimize financial operations, improve client experiences, and create better products.

Financial service firms face a number of issues, including increased expenses, more demanding consumers, and disruptive innovations. As smaller companies use technologies like blockchain, IoT, and AI to reimagine the client experience, the financial services sector is undergoing a significant transformation. These developments have the potential to seriously upend established players in the future. Established insurers, on the other hand, maintain a competitive advantage because of long-standing client relationships, substantial expertise, and access to important data from their operations, partners, and market environment.

Blockchain has the potential to completely transform the way financial services organizations function. It can assist insurers in streamlining procedures, cutting costs, improving transparency, guaranteeing legal compliance, and developing better markets and products.

By speeding up claims processing and settlements while maintaining equity and transparency, blockchain technology revolutionises the insurance industry. Its decentralised architecture reduces inefficiencies by improving fraud detection, streamlining underwriting, and facilitating seamless client onboarding. Businesses may establish a competitive edge, grow their networks, and foster trust by incorporating blockchain components. Increased customer happiness, improved operational efficiency, and more accurate risk assessments are the results of this invention, which opens the door for the industry to continue growing and developing.

2. LITERATURE REVIEW
Authors Castro et al., in [1] explore hybrid consensus models that combine multiple mechanisms to address the weaknesses of individual approaches. The authors state an example for a PoW/PoS hybrid combination for the security of PoW with the energy efficiency of PoS, aiming to offer a balance between security and scalability. Another example is Practical Byzantine Fault Tolerance (PBFT), which is also discussed, which provides robust security and reliability in permissioned networks but faces scalability and resource intensity issues in large networks. Authors in [1] also state the limitation of this hybrid model is the increase in operational complexity and present security trade-offs. PBFT struggles with scalability and resource consumption in large networks. Blockchain solutions provide scalability solutions focused on increasing transaction throughput. Sharding (Zhang et al., 2019) divides the blockchain into smaller partitions (shards) that can process transactions in parallel, reducing congestion. Off-chain solutions like state channels allow transactions to be processed outside the main blockchain, reducing load but relying on trust between participants.

Author Zhang et al. state in[2] that sharding faces cross-shard communication issues and potential security vulnerabilities. Off-chain solutions can result in a lack of finality and trust issues were stated as limitation in this model.

Expert Chen, et al. in [3] demonstrate Decentralized Finance (DeFi) and Smart Con- tracts, DeFi platforms use smart contracts to offer decentralized financial services like lending, borrowing, and trading without intermediaries. These platforms provide bene- fits such as lower fees, greater transparency, and global access. However, the complexity of smart contracts introduces risks related to security vulnerabilities and scalability limitations, particularly during periods of high transaction volumes. DeFi faces scalability issues, especially on Ethereum, leading to high transaction fees. Smart contracts are prone to bugs and security exploits, risking financial losses [3].

The author; T. A. Syed; of [4] To ensure openness, security, and trust, the study presents a blockchain-based system for tracking the life cycle of vehicles. A permissioned blockchain is used by the system to connect manufacturing, ownership transfer, inspection, insurance, leasing, accident management, and disposal. Dynamic access control and real-time vehicle monitoring are made possible by IoT devices. The framework, which is implemented using Hyperledger Fabric, uses RAFT consensus for fault tolerance and smart contracts (chaincode) for automation. Used car values are estimated via a price prediction module that uses machine learning. A case study from Saudi Arabia shows how to integrate with regional laws and vehicle management procedures. The performance study validates improved scalability, security, and efficiency, allowing the system to be used globally. Tamper-proof records, fraud prevention, and smooth multi-stakeholder transactions

are all guaranteed by the blockchain.

In this paper [5], author Ankit Kumar et al. examines blockchain consensus algorithms, focusing on transaction validation, security, and scalability challenges. It analyzes both traditional and modern mechanisms, including PoW, PoS, PBFT, Bitcoin-NG, ByzCoin, and WBFT. Scalability concerns such as block size limits, computational demands, and network latency are explored. Various solutions are classified into on-chain optimizations, off-chain methods, and enhanced consensus protocols. Additionally, this paper presents a comparative analysis of throughput, node scalability, and fault tolerance. Covered applications include supply chains, healthcare, smart grids, and IoT. Improving scalability remains essential for wider blockchain adoption.

The expert of [6] K. Kapadiya, presents a blockchain- and AI-based system for detecting fraud in healthcare insurance by enhancing transparency and security. Traditional health insurance claim (HIC) systems suffer from fraud, manual verification inefficiencies, and centralized vulnerabilities. Blockchain ensures tamper-proof record-keeping, while AI and machine learning (ML) detect fraudulent claims using supervised, unsupervised, and hybrid models. Smart contracts automate claim verification, reducing human intervention and improving efficiency. A wearable-based fraud detection approach is proposed, using IoT devices to validate medical events in real-time. Security challenges, including data privacy, cyber threats, and fraudulent claim patterns, are analyzed. Scalability, standardization, and skilled professionals are critical for effective fraud detection. The proposed AI-blockchain framework strengthens trust, automation, and fraud prevention in healthcare insurance, offering a secure and scalable solution.

The study performed in [7] examines blockchain applications in healthcare supply chains with an emphasis on efficiency, security, and transparency. Key use cases such as electronic health records (EHRs), drug traceability, insurance fraud prevention, and remote patient monitoring are highlighted in a systematic literature review that examines 124 research papers. Blockchain lowers the prevalence of fake medications and guarantees safe, decentralized data sharing. High implementation costs, data privacy concerns, and regulatory obstacles are among the difficulties. In order to improve healthcare supply chain management, stakeholders and policymakers can benefit from the study's exploration of blockchain's integration with IoT, AI, and smart contracts.

A blockchain-based system study is examined by authors of [8] for safe and transparent prescription medication health insurance claims. By automating registration and claim approval through a private Ethereum blockchain with smart contracts, fraud and inefficiencies are decreased. Data security is guaranteed by IPFS off-chain storage, and accessibility is enhanced by DApps. By creating a tamper-proof network between insurers, pharmacies, and medical providers, the system improves automation, transparency, and confidence. Improved privacy, fraud prevention, and scalability over conventional systems are confirmed by security studies. Healthcare claim processing is streamlined by this decentralised framework, which guarantees accuracy while cutting expenses.

According to the paper, Digi_s authored by U. Khan, et al. in [9] is a blockchain-based system that shares and trades digital content on an Ethereum-powered blockchain. The aim is to increase security, transparency, and trust in the sharing economy. It is built on Ethereum and automates the transactions between content providers and users, reducing dependence on intermediaries and limiting fraud. It uses SHA-256, Merkle trees, and MD5 hashing to protect digital content from forgery or hacking using encryption of the information (both real and digital). The system also provides a trust evaluation feature that allows users to rate each other and increase the authenticity of an agreement within the contract. Its implementation is based on Solidity, Geth, and the Ethereum Virtual Machine (EVM) and runs on a private network to test its performance. Test results indicate that the system is capable of verifying transactions against hacking attempts and safeguarding content sharing. Nevertheless, the authors recognise difficulties such as scalability and execution speed, noting that future developments could be more efficient.

The paper[10] by A. A. Alhussayen, K. Jambi, M. Khemakhem and F. E. Eassa presents a blockchain oracle-based interoperability technique tailored for permissioned blockchains, specifically Hyperledger Fabric and Corda. As interoperability is vital for enabling secure data exchange and cross-network smart contract invocation in enterprise applications, the authors address a gap in current research—where oracles haven't been explored for permissioned blockchain interoperability. The proposed system is easy to integrate and maintains decentralization by embedding oracle nodes within each blockchain network. A prototype implementation demonstrates the system’s feasibility, with cross-network transaction latency evaluated against local transactions. Results show a slight latency increase in Corda and a larger, but expected, increase in Hyperledger Fabric due to its interaction with Corda. Overall, the approach enables secure, decentralized data exchange and business operations across private blockchains, offering a promising solution to existing limitations.

The paper named [A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework] by M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin and M. Al-Amin in [11] offers a comprehensive analysis of blockchain architecture, covering its five core layers data, network, agreement, smart contracts, and operation. It serves as a reference companion for understanding each subcaste’s part and helps compendiums choose the applicable algorithms, protocols, and tools grounded on specific use cases. Special emphasis is placed on agreement mechanisms, pressing their impact on sustainability and energy consumption. Through simulations and relative analysis, the study evaluates trade-offs in scalability, decentralization, and performance. The exploration presents a taxonomy-grounded frame for assaying blockchain systems and supports the development of effective, secure, and customised blockchain platforms. It bridges theoretical generalities with real-world operations, aiming to support inventors, experimenters, and diligence in erecting coming-generation decentralized systems across sectors like finance, healthcare, and force chains.

A comprehensive review of distributed ledger technologies (DLTs), focusing on blockchain and its consensus mechanisms is presented in [12]. Analyzing 185 sources and 130 consensus algorithms, the study introduces a novel classification system based on the core components of consensus protocols. These are grouped into eight categories, including Primitive, Proof Compliant, BFT Compliant, Hybrid, and Extension types. The classification provides a structured way to compare algorithms based on their communication models and design features, offering insights into their functionality, advantages, and limitations. The paper also analyzes how these categories are distributed across major blockchain application domains such

as cryptocurrency, supply chain, and healthcare. The study concludes that Pure Alternatives (PA), Proof Compliant Extensions (PCE), and BFT Compliant Extensions (BCE) are the most widely adopted consensus types. It emphasizes the importance of consensus evolution for the future of DLTs and offers a solid framework for further research and development.

The paper [13] presents a comprehensive survey of blockchain technology, covering its evolution, architecture, development frameworks, consensus algorithms, security risks, and cryptographic foundations. Unlike other surveys that focus on limited aspects, this work offers an integrated analysis of blockchain's core components along with a comparative study of existing frameworks and consensus mechanisms. It also highlights the technology's potential to transform industries beyond finance, much like how the internet revolutionized communication. Additionally, the paper reviews past research contributions, identifies their limitations, and outlines future research directions and open challenges, encouraging innovation in areas like smart contracts, privacy, and decentralized applications. It serves as a foundational reference for both researchers and developers aiming to explore or improve blockchain systems.

Blockchain-based applications have gained popularity due to their reduced reliance on a central authority, but achieving consensus across blockchain networks remains a critical and complex challenge. Authors of [14] offer an extensive study of various consensus algorithms used in different blockchain systems, highlighting their strengths and limitations. It compares these protocols in terms of performance, transaction cost, and scalability, showing that no single algorithm is best for all scenarios—selection depends on specific application needs. The study also examines operational and interoperability challenges, emphasizing issues like security, efficiency, and scalability. By analyzing these factors, the paper provides valuable recommendations for developers to design more reliable and interoperable blockchain systems, making it a useful guide for future research and development.

Blockchain technology has made notable strides recently, showing promise to transform education by enabling secure, cost-effective learning and collaboration. One key application is the issuance and verification of immutable digital academic certificates, which improves speed, reliability, and independence from central authorities.The study done by authors in [15] have systematically reviewed 34 relevant articles (from an initial 1744 between 2018-2022) focusing on blockchain-based academic credential verification. Six major themes emerged: blockchain categorization, automatic certificate generation, security and transparency, adapting architectures, forgery prevention, and conceptual frameworks. Despite growing interest, challenges remain, including high maintenance costs, lack of expertise, identity verification, and data management. The paper offers future research directions to help overcome these obstacles and supports further blockchain adoption in education.

Blockchain technology is gaining interest in healthcare for addressing challenges in Electronic Health Records (EHR) systems, especially issues of trust, privacy, and security. This study reviewed in paper [16] reviews 143 blockchain-in-healthcare articles, focusing on 61 prototypes and implementations. It found that while blockchain improves security and trust, it faces challenges with scalability, cost, and performance. Most work is still experimental, with key use cases in data sharing, access control, and auditing across various health domains. Future research should focus on better performance metrics and data management to enable wider adoption. This review offers useful insights for stakeholders exploring blockchain in healthcare.

An etherium based platform was implemented by experts in [17] they state that Smart cities must prioritize citizen safety, healthcare, and data privacy, especially as Electronic Health Records (EHRs) face growing cyber threats. The integration of financial data with health insurance policies increases security concerns, as fraudulent access could alter sensitive information. Patients also face repeated identity verification across different healthcare providers, adding to their challenges. To address these issues, a blockchain-based healthcare platform using Ethereum is proposed, which secures patient data and insurance policies through cryptographic tools. The system includes key entities like patients, hospitals, insurance companies, and cloud storage, ensuring data transparency and secure sharing. Healthcare records are stored in the cloud, while identity and insurance data are protected on the blockchain. The platform's implementation shows its effectiveness and future plans include data aggregation to predict public health trends—particularly valuable during events like COVID-19.

[18] explores the deployment of blockchain technology in telecommunications, focusing on key challenges like cost, scalability, and performance. It examines different infrastructure options—on-premises, Infrastructure-as-a-Service (IaaS), and Blockchain-as-a-Service (BaaS)—by analyzing two primary use cases: 5G slice brokering and federated learning (FL). Experiments reveal that slice brokering can achieve sub-second latency and up to 200 TPS with moderate resources, while FL benefits from private or consortium blockchains for faster training and better accuracy. The study highlights how block size, batch size, and inter-block time affect FL performance, revealing trade-offs in accuracy and scalability. Additionally, the research outlines five telecom use cases for blockchain and evaluates each against performance, cost, and regulatory requirements. While larger block sizes improve FL model accuracy, their feasibility in high-frequency, large-node environments remains uncertain. The article provides a foundation for cost-performance analysis and emphasizes the need for further research to support massive-scale applications like IoT and V2V, ensuring privacy compliance and operational efficiency.

This study performed in [19] explores the role of blockchain technology in addressing development challenges during pandemics, particularly in the context of developing countries under the ICT4D framework. The COVID-19 crisis has intensified existing problems in health, digital identity, supply chain traceability, and aid transparency, highlighting the potential of blockchain as a disruptive and transformative tool. While still maturing, blockchain offers opportunities for more efficient vaccine distribution, hotspot tracking, and corruption prevention. However, challenges like political instability, lack of infrastructure, and technological readiness must be addressed. The paper stresses the importance of careful implementation, ethical responsibility from the Global North, and investment in technology and policy frameworks. It provides insights for governments, NGOs, scholars, and industries to harness blockchain effectively for present and future pandemics.

This study examined in [20] explores the potential of blockchain technology in the healthcare sector, especially in supply chains. Blockchain's features—such as security, transparency, and traceability—can address major issues like

fragmented records, drug counterfeiting, and insurance fraud. Through a systematic literature review of 124 papers, it finds that most research is still in early stages and largely theoretical. India is the most active country in this field, and IEEE Access is the top publishing journal. Key applications include EHR management, remote monitoring, and medical insurance. However, adoption faces challenges like high costs, security concerns, interoperability issues, and limited trust. Despite these hurdles, blockchain holds promise for digitizing healthcare and building trust among stakeholders. The study provides a roadmap for future research and practical adoption strategies.

The paper [21] paper introduces Concordia, a novel Byzantine fault-tolerant consensus protocol designed for sharded blockchain systems. Unlike traditional leader-driven models, Concordia uses a single block proposer per round and leverages threshold signatures for secure and efficient block validation. By adopting a gossip-like communication pattern, nodes can collect and verify group signatures in O(logN) steps, allowing block finality to be achieved with just one round of one-way communication. This design prevents forks and ensures both safety and liveness, even with up to f faulty nodes in a network of 2f + 1 participants. The protocol's efficiency is demonstrated through a prototype implementation, which achieves approximately 2,000 transactions per second and a block confirmation latency of around 10 seconds, even in large networks. Concordia's tightly integrated components—proposer selection, gossip messaging, and BLS threshold signatures—enable high throughput and scalability. Its architecture makes it particularly suitable for intra-shard consensus in high-performance blockchain systems, ensuring secure and scalable transaction processing with minimal latency.

Experts in [22] propose DApp for the healthcare sector is rapidly evolving, with growing demands for better patient care, regulatory compliance, and digital transformation. Telemedicine has emerged as an affordable and effective solution but faces challenges such as data breaches, limited access, incorrect diagnoses, and fraud. To address these issues, this paper proposes a blockchain-based telemedicine framework using Ethereum smart contracts, which ensures transparency, data integrity, and decentralization by eliminating the need for a central administrator. The smart contracts regulate interactions between stakeholders and keep patients informed about every transaction. The framework also includes automated claim settlements by medical insurers, enhancing efficiency and trust. Any entity within the healthcare network can verify transactions, ensuring secure transfer of sensitive data. This decentralized system improves accessibility and accountability in remote healthcare services. The solution is initially developed in the Remix IDE and is planned for future deployment on the Hyperledger network. Additionally, Decentralized Applications (DApps) will be created to provide user-friendly interfaces for patients, physicians, and insurers.

This paper[23] introduces a novel consensus algorithm called Delegated Proof of Stake with Downgrade (DDPoS), which combines the computational strength of Proof of Work (PoW) with the efficiency of Delegated Proof of Stake (DPoS) to enhance fairness, decentralization, and security. By reducing dependence on computational resources and stake size, DDPoS achieves better performance in block generation while maintaining low resource consumption. A key innovation is the downgrade mechanism, designed to detect and swiftly replace malicious nodes, ensuring stable and secure network operations. Nodes are limited to one random vote each, discouraging collusion and promoting fairness in leader selection. Simulation results demonstrate that DDPoS outperforms PoW and PoS in efficiency, while achieving greater decentralization than DPoS. The system increases node activity and security through improved participation incentives and rapid response to threats. Although testing is currently limited to a simulated environment, future work aims to apply DDPoS to real-world blockchain platforms such as Hyperledger and Ethereum.

Authors in [24] analyze 696 blockchain articles in Business and Management published between 2015 and 2021 using CiteSpace and VOSviewer tools. It identifies four foundational research themes and highlights global contributions from leading journals, authors, and countries. The major research hotspots include finance and risk management, organizational transformation, and the integration of artificial intelligence. Blockchain research has evolved from a focus on cryptocurrency to broader impacts on business ecosystems. However, the study is limited by reliance on a single database and lacks dynamic co-citation analysis. Future research should explore how blockchain challenges traditional business and management theories and develop new data processing methods suited for decentralized storage systems.

In [25] experts explore the development of Mobile Smart Contracts (MSCs) by analysing scalability challenges and consensus mechanisms through a systematic literature review (SLR) of 2,073 studies, with 25 selected for in-depth analysis. It identifies 12 consensus mechanisms and 13 scalable blockchain systems, revealing that no current solution fully supports the lightweight, scalable requirements for MSCs. The Proof of Stake (PoS) mechanism emerges as a promising approach due to its scalability, though issues like oligopoly formation and the nothing-at-stake problem persist. Sharding is evaluated for its potential but suffers from inefficient cross-shard communication, small shard sizes, and lack of strong resiliency. Key contributions include a classification of scalability strategies, analysis of sharding protocols, and identification of scalable consensus algorithms. The paper concludes that advancing scalable and energy-efficient blockchain protocols is essential for enabling smart contracts on mobile devices. Future work will focus on integrating PoS with sharding to validate MSC transactions, offering guidance to researchers, developers, and users in addressing blockchain scalability and security for mobile environments.

This paper[26] introduces Proof of Random Leader (PoRL), a novel Proof of Authority (PoA)-based consensus algorithm designed for permissioned blockchain networks. PoRL addresses key limitations of traditional PoA variants like Aura and Clique, which suffer from low throughput, predictable leader selection, and vulnerability to timing attacks. By incorporating a Verifiable Random Function (VRF), PoRL ensures fair, unpredictable leader election, enhancing both security and scalability. The algorithm, implemented in Python and tested on six heterogeneous nodes, was evaluated against key metrics: consensus time, transaction throughput, availability, and fault tolerance. Results show PoRL achieves faster consensus and higher throughput than Aura and Clique, while Clique provides greater availability and Aura ensures better security. The study highlights that no single algorithm is ideal for all use cases, offering practical guidance for blockchain practitioners. Future research will explore PoRL's performance across larger, distributed environments, aiming to optimize PoA protocols for real-world deployment.

In [27], experts the 5G networking era, enforcing Secure Service Level Agreements (SSLAs) is critical for ensuring security standards like integrity, confidentiality, and availability between service providers and tenants. However, the rise of distributed, multi-stakeholder architectures introduces complexity in managing these SSLAs. To address this, the paper proposes a novel blockchain-based SSLA management framework featuring a custom consensus mechanism called Proof-of-Monitoring (PoM). PoM enhances performance by reducing energy consumption, computation cost, and latency compared to traditional mechanisms like Proof-of-Work. The framework also leverages off-chain databases to store monitoring data securely, improving scalability and adaptability. Prototype results show improved efficiency and robust security features, making it suitable for current and future network environments. Future plans include integrating AI to predict SSLA violations, enhancing proactive security and system resilience.

Experts in paper [28] examines the research methodologies used by the Smart Contracts Working Group (TC-307/IT-041) in shaping blockchain and distributed ledger technology (DLT) standards. It traces the origins of blockchain standardization and outlines a flexible, responsive research framework suited to the fast-evolving tech landscape. Through three case studies—smart contract legality, regulatory frameworks in trade and supply chains, and integration of UN Sustainable Development Goals—the paper highlights how adaptive methods improve research relevance and efficiency. It stresses the importance of balancing researcher autonomy with stakeholder collaboration to deliver practical, globally applicable findings. The research approach is not a rigid formula but a checklist emphasizing clear communication, iterative analysis, sprint-based planning, and qualified conclusions. Ultimately, the study offers practical insights for researchers contributing to international blockchain standards and emerging technologies.

Blockchain technology has gained prominence in decentralized transaction systems, particularly in cryptocurrency markets, due to its tamper-proof and distributed ledger structure. As mobile and IoT technologies advance, there's an increasing need to evaluate blockchain’s performance, data management, and storage capabilities on resource-constrained devices. Experts in [29] presents a systematic review of blockchain's design principles, analyzing Ethereum's performance across two devices with varying computing power. Metrics such as CPU usage, latency, and execution time highlight limitations in deploying blockchain on low-power processors like ARM. To support this evaluation, developed Debug-Bench, the first Visual Studio Code extension for benchmarking and profiling blockchain applications. The study identifies critical performance challenges in current platforms and proposes future research directions to bridge the performance gap for effective blockchain integration in constrained environments such as IoT.

In the era of Industry 4.0, blockchain technology serves as a transformative solution to enhance traceability, transparency, trust, and data authenticity in digital business networks. Its applications span across finance, healthcare, and supply chains by enabling secure and efficient data sharing. However, blockchain faces a fundamental trade-off between scalability, security, and decentralization. Permissionless blockchains offer strong security and decentralization but struggle with performance, while permissioned blockchains are more efficient but vulnerable to cyberattacks due to weaker consensus mechanisms. This paper [30] emphasizes the critical role of robust consensus protocols in securing blockchain systems, especially in permissioned networks prone to attacks such as Sybil, 51%, DDoS, and double spending. It analyzes existing consensus models, highlights their limitations in dynamic environments, and identifies key security threats and operational gaps. The study proposes resilient, adaptive consensus mechanisms as essential for improving security and performance. A multidimensional approach—considering both technical resilience and participant behavior—is vital. Future research must focus on scalable, secure protocols and proactive defenses, while collaboration among academia, industry, and regulators is crucial for innovation and standardization in blockchain security.

Practical Byzantine Fault Tolerance (PBFT) is widely used in blockchain consensus but suffers from high communication overhead and lacks incentives for reliable nodes. To address this, a new protocol—Credit-Delegated Byzantine Fault Tolerance (CDBFT)—is proposed. CDBFT introduces a credit-based voting, reward, and punishment mechanism to encourage reliable node participation and reduce the influence of abnormal nodes. It also enhances PBFT with optimized consistency and checkpoint protocols to improve flexibility and efficiency. Simulations performed in [31] results show CDBFT reduces abnormal node participation to 5% and significantly improves system stability, making it suitable for consortium blockchains with lower overhead.

Blockchain technology is revolutionizing industries with its core features—immutability, tamper-proofing, and verifiable data provenance—enhancing security, operational efficiency, and trust. While it has significantly impacted the financial sector, its potential in non-financial domains is rapidly expanding. This includes applications in healthcare, energy, insurance, supply chain, digital voting, and government, where blockchain addresses complex challenges. The integration of blockchain with technologies like IoT, AI, edge computing, and federated learning further amplifies its capabilities. The study explored [32] these non-financial use cases, highlighting improved data security, automation through smart contracts, and resistance to cyber-attacks, while also outlining future opportunities for broader adoption.

The Cosmos blockchain presented in [33] is a decentralized network designed to overcome scalability and interoperability challenges through the Tendermint consensus mechanism and IBC protocol. It enables secure, seamless cross-chain transactions and supports decentralized governance via the ATOM token. This study highlights Cosmos’s modular architecture and adaptability across industries like finance, healthcare, and supply chains. While it offers significant strengths, such as flexibility and scalability, challenges like security risks and architectural complexity remain. Overall, Cosmos presents a promising framework for blockchain interoperability and the advancement of decentralized applications.

Table 1. Comparative Analysis of Blockchain Consensus Mechanisms

Consensus	Year Introduced	Key Mechanism	Throughput (TPS)	Energy Efficiency	Fault Tolerance	Primary Use Cases	Limitations	Reference
PoW	2008 (Bitcoin)	Hash-based mining	3–7 (Bitcoin)	Low	**Moderate (51% attack)**	**Cryptocurrencies**	**High energy use, slow**	**[1], [5], [13]**
PoS	2012 (Peercoin)	Stake-based validation	50–100 (Ethereum 2.0)	High	**Moderate**	**DeFi, Governance**	**"Nothing-at-stake" problem**	**[5], [25], [32]**
PBFT	1999 (Original)	Voting-based agreement	1,000–10,000	High	**High (≤1/3 faulty)**	**Permissioned chains (Healthcare [4])**	**O(N²) messaging overhead**	**[1], [4], [21]**
DPoS	2014 (Bitshares)	Delegated stake voting	1,000–5,000	High	**Low (centralization)**	**High-speed transactions (EOS)**	**Centralization risks**	**[23], [5]**
PoRL	2025 [26]	VRF-based leader election	2,000+	High	**High**	**IoT, Telecom**	**Limited real-world testing**	**[26]**
Concordia	2021 [21]	Sharded BFT	2,000+	High	**High**	**Sharded blockchains**	**Complexity in implementation**	**[21]**
Tendermint	2016 (Cosmos)	BFT + PoS hybrid	1,000–10,000	High	**High**	**Cross-chain interoperability**	**Requires trusted validators**	**[33], [11]**

3. CONCLUSION

This paper provides a comprehensive analysis of blockchain agreement mechanisms and their operations in healthcare and insurance services, laying the root for designing a technical agreement protocol for Health Insurance Service Blockchain DApps . The study reveals that while agreement consensus similar as PoW, PoS, PBFT, and cold-blooded approaches — offer varying degrees of security, scalability, and decentralization, they do not address the unique demand of insurance.

The healthcare and insurance sectors present distinct conditions, including secure case data sharing, automated claim processing, and tamper-evidence inspection trails , which current blockchain executions struggle to completely satisfy. For example, PBFT ensures robustness in permissioned networks but suffers from scalability issues, while PoS-grounded systems reduce energy consumption but may introduce centralization pitfalls. Arising protocols like sharded BFT and PoRL demonstrate promising advancements in outturn and fault forbearance, yet their connection to health insurance DApps remains underexplored.

To bridge these gaps, concentrate on integrating the strengths of various mechanisms while addressing the limitations. Eventually, this check underscores the critical need for an innovative agreement frame that not only aligns with the specialised demands of blockchain-grounded insurance systems but also fosters trust, translucency, and effectiveness across the ecosystem.

4. REFERENCES

[1] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI'99).Zhang, Y., et al. (2019). Sharding-based blockchain scalability solutions: A survey. International Journal of Computer Science & Information Technology, 11(2), 47-61.

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

[3] Chen, L., et al. (2020). Security and performance analysis of decentralized finance (DeFi) protocols. Journal of Blockchain Research, 11(2), 67-92.Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[4] 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 Solution," in IEEE Access, vol. 8, pp. 111042-111063, 2020, doi: 10.1109/ACCESS.2020.3002170.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] U. Khan, Z. Y. An and A. Imran, "A Blockchain Ethereum Technology-Enabled Digital Content: Development of Trading and Sharing Economy Data," in IEEE Access, vol. 8, pp. 217045-217056, 2020, doi: 10.1109/ACCESS.2020.3041317.

[10] A. A. Alhussayen, K. Jambi, M. Khemakhem and F. E. Eassa, "A Blockchain Oracle Interoperability Technique for Permissioned Blockchain," in IEEE Access, vol. 12, pp. 68130-68148, 2024, doi: 10.1109/ACCESS.2024.3400672.

[11] M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin and M. Al-Amin, "A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework," in IEEE Access, vol. 12, pp. 63087-63129, 2024, doi: 10.1109/ACCESS.2024.3395536.

[12] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," in IEEE Access, vol. 9, pp. 43620-43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[13] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," in IEEE Access, vol. 9, pp. 61048-61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[14] S. Islam, M. J. Islam, M. Hossain, S. Noor, K. -S. Kwak and S. M. R. Islam, "A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues," in IEEE Access, vol. 11, pp. 39066-39082, 2023, doi: 10.1109/ACCESS.2023.3267047.

[15] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in IEEE Access, vol. 11, pp. 64679-64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[16] E. Chukwu and L. Garg, "A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations," in IEEE Access, vol. 8, pp. 21196-21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[17] A. A. Omar et al., "A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities," in IEEE Access, vol. 9, pp. 90738-90749, 2021, doi: 10.1109/ACCESS.2021.3089601.

[18] N. Afraz, F. Wilhelmi, H. Ahmadi and M. Ruffini, "Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis," in IEEE Access, vol. 11, pp. 95653-95666, 2023, doi: 10.1109/ACCESS.2023.3309423.

[19] S. Karnouskos, "Blockchain for Development in the Era of the COVID-19 Pandemic," in IEEE Open Journal of the Industrial Electronics Society, vol. 2, pp. 556-567, 2021, doi: 10.1109/OJIES.2021.3121549.

[20] 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.

[21] C. Santiago, S. Ren, C. Lee and M. Ryu, "Concordia: A Streamlined Consensus Protocol for Blockchain Networks," in IEEE Access, vol. 9, pp. 13173-13185, 2021, doi: 10.1109/ACCESS.2021.3051796.

[22] A. Abugabah, N. Nizamuddin and A. A. Alzubi, "Decentralized Telemedicine Framework for a Smart Healthcare Ecosystem," in IEEE Access, vol. 8, pp. 166575-166588, 2020, doi: 10.1109/ACCESS.2020.3021823.

[23] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[24] J. Yang, C. Ma, D. Li and J. Liu, "Mapping the Knowledge on Blockchain Technology in the Field of Business and Management: A Bibliometric Analysis," in IEEE Access, vol. 10, pp. 60585-60596, 2022, doi: 10.1109/ACCESS.2022.3179714.

[25] V. Deval et al., "Mobile Smart Contracts: Exploring Scalability Challenges and Consensus Mechanisms," in IEEE Access, vol. 12, pp. 34265-34288, 2024, doi: 10.1109/ACCESS.2024.3371901.

[26] M. M. Islam, M. M. Merlec and H. P. IN, "Proof of Random Leader: A Fast and Manipulation-Resistant Proof-of-Authority Consensus Algorithm for Permissioned Blockchains Using Verifiable Random Function," in IEEE Transactions on Services Computing, vol. 18, no. 3, pp. 1655-1668, May-June 2025, doi: 10.1109/TSC.2025.3536315.

[27] N. Weerasinghe, R. Mishra, P. Porambage, M. Liyanage and M. Ylianttila, "Proof-of-Monitoring (PoM): A Novel Consensus Mechanism for Blockchain-Based Secure Service Level Agreement Management," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2783-2803, Sept. 2023, doi: 10.1109/TNSM.2023.3234862.

[28] M. Maslin, M. Watt and C. Yong, "Research Methodologies to Support the Development of Blockchain Standards," in Journal of ICT Standardization, vol. 7, no. 3, pp. 249-268, 2019, doi: 10.13052/jicts2245-800X.734.

[29] M. Imran et al., "Research Perspectives and Challenges of Blockchain for Data-Intensive and Resource-Constrained Devices," in IEEE Access, vol. 10, pp. 38104-38122, 2022, doi: 10.1109/ACCESS.2022.3162096.

[30] N. M. Nasir, S. Hassan and K. Mohd Zaini, "Securing Permissioned Blockchain-Based Systems: An Analysis on the Significance of Consensus Mechanisms," in IEEE Access, vol. 12, pp. 138211-138238, 2024, doi: 10.1109/ACCESS.2024.3465869.

[31] Y. Wang et al., "Study of Blockchains's Consensus Mechanism Based on Credit," in IEEE Access, vol. 7, pp. 10224-10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[32] C. Vanmathi, A. Farouk, S. M. Alhammad, R. Mangayarkarasi, S. Bhattacharya and M. S. B. Kasyapa, "The Role of Blockchain in Transforming Industries Beyond Finance," in IEEE Access, vol. 12, pp. 148845-148867, 2024, doi: 10.1109/ACCESS.2024.3468611.

[33] M. S. Peelam, B. K. Chaurasia, A. K. Sharma, V. Chamola and B. Sikdar, "Unlocking the Potential of Interconnected Blockchains: A Comprehensive Study of Cosmos Blockchain Interoperability," in IEEE Access, vol. 12, pp. 171753-171776, 2024, DOI: 10.1109/ACCESS.2024.3497298.