IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

A Review on Distributed Computational Network on a Peer to Peer Blockchain

Sujan Reddy[1] and T N Sai Krishna[1]
B.E. Students, Department of Information Science and Engineering
Global Academy of Technology, Bangalore, India

Abstract: *The survey outlines the implementation of a Decentralized Computational Network (DCN) using a peer-to-peer blockchain infrastructure. The focus is on overcoming centralization challenges such as scalability issues and security concerns. The study introduces dynamic load balancing, peertopeer consensus mechanisms, and smart contracts for decentralization and scalability. Additionally, it explores homomorphic encryption for enhanced privacy and a novel tokenomics-based incentive structure to encourage active participation in the DCN. This research contributes a concise yet comprehensive technical architecture for a resilient and efficient decentralized computational network*

Keywords: Transparency, Trustlessness, Dynamic Load Balancing, Incentive Mechanism, Peertopeer Consensus, Smart Contracts, Homomorphic Encryption

I. INTRODUCTION

In an era dominated by technological advancements, the pursuit of computational efficiency has become a paramount objective across various industrial sectors. The seamless integration of cutting-edge technologies not only promises heightened productivity but also holds the potential to significantly reduce operational costs, fostering an environment of increased competitiveness. Simultaneously, the paradigm of decentralization emerges as a catalyst for societal empowerment, offering individuals unprecedented access to computational resources. This decentralized approach not only cultivates inclusivity but also acts as a breeding ground for innovation across diverse societal domains.

Amidst this technological landscape, concerns about privacy and security have grown exponentially, particularly in the context of data handling and processing. Recognizing the urgency to address these issues, our project places a strategic focus on leveraging blockchain technology and homomorphic encryption. This dual-pronged approach is designed to not only meet the critical needs of secure and private computational processes but also align with the broader societal and industrial imperatives. As we embark on this journey to enhance computational efficiency and empower societies through decentralization, our commitment lies in navigating the intersection of technology and societal needs, forging a path toward a more resilient and progressive future.

II. DECENTRALIZATION TECHNIQUES

Decentralization techniques encompass a range of strategies aimed at redistributing authority and control across networks or systems. Blockchain technology, a foundational element, establishes a decentralized and tamper-resistant ledger for transactions and information. Peer-to-peer networks enable direct communication and resource sharing between nodes, eliminating the need for a central server. Distributed consensus mechanisms, such as Proof-of-Work and Proof-of-Stake, decentralize transaction validation and block creation. Smart contracts automate contractual processes on blockchain platforms, removing the need for centralized intermediaries. Federated systems delegate authority to multiple entities while maintaining some control at the system level.

Mesh networks enhance reliability by allowing devices to connect directly. Decentralized Autonomous Organizations (DAOs) distribute decision-making among participants through coded rules and voting mechanisms. InterPlanetary File System (IPFS) facilitates peer-to-peer content distribution, reducing reliance on centralized servers. Homomorphic encryption ensures privacy during decentralized computations. Tokenization and cryptocurrencies enable decentralized transactions and incentivize network participants. Collectively, these decentralization techniques contribute to building resilient, transparent, and trustless systems across diverse domains, ushering in a new era of decentralized innovation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.1 Incentive Mechanisms in Peer-to-Peer Networks — A Systematic Literature Review

This study, titled "Incentive Mechanisms in Peer-to-Peer Networks — A Systematic Literature Review," conducted by Cornelius Ihle, Dennis Trautwein, Moritz Schubotz, Norman Meuschke, and Bela Gipp, explores the role of incentive mechanisms in decentralized networks. The authors emphasize the importance of decentralization in mitigating single points of failure present in centralized systems. The study systematically reviews 165 literature reviews and 178 primary research papers published between 1993 and October 2022, providing a comprehensive analysis of incentive mechanisms for decentralized networks and systems.

The study categorizes and compares distinctive properties of incentive mechanisms, such as fairness, participation, and cooperation rewards. Three incentive categories—monetary, reputation, and service—are evaluated across various network types, including Opportunistic Networks, Mobile Ad-Hoc Networks, and Delay-Tolerant Networks. The authors highlight the critical role of decentralized computation, specifically employing smart contracts combined with distributed ledgers, in maintaining incentive mechanisms without a central authority. The study identifies research gaps, deficiencies in reproducibility and comparability, and concludes by offering recommendations for the application of incentive mechanisms in decentralized networks sharing computational resources. The comprehensive literature review aims to support the research and development of decentralized Peer-to-Peer systems, providing valuable insights into the design aspects of incentive mechanisms.

Advantages: Enhanced resilience and security in decentralized networks with incentive mechanisms.

Disadvantage: Implementation complexity and historical dependencies on central authorities in decentralized Peer-to-Peer networks.

2.2 Simulation of a secure approach of data communication of peer to peer network using blockchain network using blockchain technology on Ethereum

This study explores the implementation of a secure data communication approach on a peer-to-peer network using blockchain technology on Ethereum. Authored by Ms. Rohaila Naaz and Dr. Ashendra Kumar, The study addresses the need for enhanced security in social media networks and instant messaging, emphasizing the limitations of current end-to-end encryption (E2EE) implementations. The authors propose integrating blockchain, leveraging its characteristics of data integrity, immutability, and anonymity, to address privacy and security concerns. The study includes a simulation comparing the existing E2EE using AES 256 in Python with a blockchain-enabled secure messaging system implemented in Solidity.

Results demonstrate comparable power consumption and memory usage, highlighting the potential of blockchain in securing communication in peer-to-peer networks. The study underscores the relevance of blockchain in achieving the motivations of E2EE, emphasizing privacy, data control, and security.

Advantage: The integration of blockchain technology enhances the security of data communication in peer-to-peer networks by providing features such as data integrity, immutability, and anonymity. This ensures that messages exchanged over the network remain secure and tamper-proof, addressing privacy and security concerns more effectively than traditional encryption methods.

Disadvantage: Implementing blockchain-enabled secure messaging systems may introduce additional complexity and overhead compared to traditional end-to-end encryption (E2EE) implementations. This complexity can lead to higher development costs and potential challenges in adoption and integration into existing communication platforms.

2.3 Load Balancing Framework for Cross-Region Tasks in Cloud Computing

The study, titled "Load Balancing Framework for Cross-Region Tasks in Cloud Computing," explores the integral role of load balancing in the cloud computing landscape, specifically focusing on tasks spanning multiple regions. Addressing the surge in data volume and heightened internet usage, The study introduces an innovative approach to load balancing at the database level. Various algorithms and techniques are examined to efficiently distribute computing tasks, emphasizing the importance of maintaining effective task scheduling processes and optimizing resource utilization.

Through scenario-based results, The study highlights the tangible benefits of load balancing, particularly in managing cross-regional traffic and enhancing revenue growth for restaurants. In the broader context of cloud computing, The

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

study underscores the technology's rapid growth, offering Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Visual representations in Figure 1 illustrate interconnected load balancing groups, showcasing their controlled interaction through a database. The study showcases the advantages of load balancing, including streamlined cloud resource utilization, fair computing resource allocation, and the prevention of user access issues.

It further explores automatic scaling listeners and proposed load balancing algorithms, demonstrating their contributions to improved access times in diverse regions. The findings underscore the cost-efficiency and revenue-generation benefits of load balancing, particularly evident in the restaurant industry for the year 2020.

Advantage: The study introduces an innovative approach to load balancing at the database level, which effectively distributes computing tasks across multiple regions in cloud computing environments. By optimizing resource utilization and maintaining efficient task scheduling processes, the proposed framework ensures streamlined cloud resource utilization, fair computing resource allocation, and prevents user access issues, leading to improved performance and user experience.

Disadvantage: Implementing load balancing frameworks and algorithms, especially at the database level, may require significant development efforts and investments in infrastructure. Additionally, the complexity of managing load balancing across multiple regions and integrating it into existing cloud computing architectures can pose challenges for organizations, potentially leading to higher operational costs and technical hurdles.

2.4 Blocktree: A Distributed Computing Environment

Blocktree is proposed as a distributed computing environment based on the actor model, designed to extend the Unix philosophy to the entire distributed system. The system features a global distributed filesystem with strong security measures, utilizing TLS authentication, a trust model, and cryptographic protections for data integrity and confidentiality. Its innovative approach includes a Raft consensus protocol for high availability, a self-certifying filesystem structure with delegated authority, and a session typing system to facilitate the creation of composable distributed systems. Implemented in Rust and tested on Linux, Blocktree aims to empower users to host their own services, offering flexibility in cloud computing and a zero-trust approach to secure communication.

The document emphasizes Blocktree's potential to address issues in current IT systems, promoting data certification by path, authenticated communication between processes, and user-friendly hosting of services. It positions Blocktree as a solution to the challenges posed by centralized cloud services, offering a platform that enhances security, flexibility, and user control in a distributed computing landscape.

Advantage: Blocktree offers a comprehensive solution to address the limitations of current IT systems by providing a distributed computing environment based on the actor model. With features like a global distributed filesystem, TLS authentication, and cryptographic protections, Blocktree prioritizes security and data integrity while empowering users to host their own services. Its innovative approach, including a Raft consensus protocol and self-certifying filesystem structure, enhances high availability and delegated authority, fostering a zero-trust approach to secure communication.

Disadvantage: Implementing and deploying Blocktree may require significant technical expertise, especially considering its use of advanced cryptographic techniques and its reliance on Rust programming language. Additionally, transitioning to a decentralized computing environment may involve challenges related to compatibility with existing systems and workflows, potentially leading to resistance from organizations accustomed to centralized cloud services.

2.5 Secure and Versatile Decentralized Ledger System Based on Blockchain for P2P Communication

The study titled "Secure and Versatile Decentralized Ledger System Based on Blockchain for P2P Communication" introduces a comprehensive framework designed to enhance secure peer-to-peer communication using blockchain technology. Addressing challenges in centralized data sharing systems, the framework eliminates the need for third-party authentication, providing increased security while saving time and costs.

Through a proof of concept in the healthcare sector, the system ensures immediate access to relevant information while securing patient health records through encryption and access controls. The study anticipates the disruptive potential of blockchain technology across various fields and proposes a versatile framework applicable to diverse types of data,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

including patient records and laboratory information. Future developments may explore alternative blockchain technologies and additional features, such as patient data validation, to further enhance the system's capabilities.

Advantage: The framework introduced in The study offers enhanced security and versatility in peer-to-peer communication by leveraging blockchain technology. By eliminating the need for third-party authentication, it not only increases security but also saves time and costs associated with centralized data sharing systems. Through a proof of concept in the healthcare sector, the system demonstrates immediate access to relevant information while ensuring the security of patient health records through encryption and access controls.

Disadvantage: Implementing a decentralized ledger system based on blockchain may introduce complexities and require significant technical expertise, potentially posing challenges for organizations unfamiliar with blockchain technology. Additionally, while the framework shows promise in the healthcare sector, its applicability to other fields and types of data needs to be further explored and validated. Future developments may also encounter scalability issues or interoperability challenges when integrating with existing systems and technologies.

2.6 Decentralized file storing and sharing system

AThe study titled "Decentralized File Storing and Sharing System" addresses the challenges associated with the storage of large files on the blockchain and introduces a novel solution leveraging the Inter-Planetary File System (IPFS). Unlike traditional blockchain systems that may encounter issues with data bloating, the IPFS offers a content-addressable distributed file system, providing a decentralized and efficient approach to file storage. The research focuses on the development of a secure file-sharing system by integrating a permission-less blockchain and IPFS, utilizing the IPFS proxy for distributed access control and group key management.

This innovative system allows members to establish or join groups based on their preferences, with access control policies ensuring that file access is restricted to authorized groups. The study underscores the inherent advantages of blockchain, emphasizing its decentralized nature, immutability, and trackability, which collectively contribute to creating a trusted transaction environment. The strategic combination of blockchain and IPFS addresses the limitations of each technology, resulting in a tamper-proof model for secure file sharing.

The proposed system not only leverages provenance data stored in the blockchain for analytical insights but also ensures traceability of file ownership and safeguards against malicious modifications. In essence, the research aims to establish a universal decentralized cloud file storage and sharing platform that significantly improves retrieval efficiency and guarantees data security.

Advantage: The proposed system offers a decentralized and efficient approach to file storage and sharing by leveraging the Inter-Planetary File System (IPFS) in conjunction with a permission-less blockchain. Unlike traditional blockchain systems that may face issues with data bloating, the IPFS provides a content-addressable distributed file system, addressing scalability concerns and ensuring efficient storage of large files. By integrating IPFS with blockchain technology, the system achieves enhanced security and accessibility, allowing users to establish or join groups with access control policies, thereby restricting file access to authorized groups.

Disadvantage: Implementing a decentralized file storing and sharing system using blockchain and IPFS may introduce complexities in terms of system architecture, configuration, and management. Integration with existing infrastructure and technologies could pose interoperability challenges, potentially hindering seamless adoption and usage. Moreover, while the system addresses scalability concerns associated with traditional blockchain systems, it may still encounter performance limitations when handling a large volume of file-sharing transactions. Additionally, ensuring the security and integrity of the system against potential vulnerabilities or attacks requires ongoing monitoring and maintenance, which could be resource-intensive.

2.7 A Review of Blockchain Platforms Based on the Scalability, Security, and Decentralization Trilemma

The study titled "A Review of Blockchain Platforms Based on the Scalability, Security, and Decentralization Trilemma" provides a comprehensive analysis of popular blockchain platforms, considering essential factors like scalability, security, and decentralization. One notable advantage highlighted in the study is the immutable nature of blockchains, ensuring enhanced security and privacy in decentralized and trusted storage systems across various sectors, including Banking, Finance, Healthcare, Government, and Supply Chain Management.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

However, a notable disadvantage emphasized in The study is the persistent challenge posed by the blockchain trilemma itself. While blockchain platforms strive to optimize scalability, security, and decentralization, achieving a perfect balance among these three factors remains a complex and evolving task. The inherent trade-offs in addressing one aspect often impact the others, making it challenging to find a universally optimal solution that satisfies all criteria simultaneously. This ongoing struggle poses a significant hurdle in designing blockchain systems that cater to diverse information system architectures effectively.

Advantage: The study highlights the immutable nature of blockchains as a significant advantage, ensuring enhanced security and privacy in decentralized storage systems across various sectors. This feature contributes to establishing trust and reliability in blockchain platforms, making them suitable for critical applications in Banking, Finance, Healthcare, Government, and Supply Chain Management. By providing a tamper-proof and transparent ledger, blockchains offer a robust solution for securely storing and managing sensitive data, thereby addressing concerns related to data integrity and unauthorized access.

Disadvantage: The persistent challenge posed by the blockchain trilemma is a notable disadvantage discussed in The study. While blockchain platforms aim to optimize scalability, security, and decentralization, achieving a perfect balance among these three factors remains a complex task. The inherent trade-offs involved in prioritizing one aspect often lead to compromises in the others, creating challenges in designing blockchain systems that effectively cater to diverse information system architectures. This ongoing struggle underscores the need for continuous innovation and refinement in blockchain technology to address the evolving requirements of various applications effectively.

2.8 Monitoring Peer-to-Peer Botnets: Requirements, Challenges, and Future Works

The study titled "Monitoring Peer-to-Peer Botnets: Requirements, Challenges, and Future Works" addresses the growing threat of cybercriminals using Peer-to-Peer (P2P) networks to establish and control botnets, which poses significant challenges for monitoring and countering these malicious activities. The study emphasizes the evolved architecture of P2P botnets, leveraging the decentralized nature of P2P networks to enhance resilience and stealthiness against conventional takedown procedures.

The monitoring of P2P botnets becomes a crucial mission, considering the need to simultaneously address challenges related to existing monitoring approaches, the unique nature of P2P networks, and the countermeasures employed by botnets to evade detection. The study categorizes monitoring approaches into passive, active, and hybrid, providing an exhaustive review of each approach's advantages and disadvantages.

Efficient monitoring is highlighted as a key factor in countering P2P botnets, as it offers insights into the botnet's structure, vulnerabilities, and communication protocols. The study emphasizes the importance of accurate monitoring for making informed decisions to mitigate the risks associated with P2P botnets. The challenges in P2P botnet monitoring are discussed, and The study concludes by outlining future avenues to enhance the monitoring of P2P botnets, emphasizing the need for more efficient and accurate approaches to combat evolving cyber threats.

Advantage: The study provides a comprehensive overview and categorization of existing monitoring approaches for P2P botnets, shedding light on their advantages and disadvantages. This categorization into passive, active, and hybrid monitoring approaches contributes to a structured understanding of the diverse strategies employed in countering P2P botnets.

Disadvantage: While The study extensively discusses monitoring approaches, it may benefit from further exploration of real-world case studies or practical implementations to validate the effectiveness of these approaches in dynamic and evolving cyber threat landscapes. Practical examples could enhance the applicability and reliability of the proposed monitoring strategies.

2.9 Blockchain-Based Secure and Trusted Distributed International Trade Big Data Management System

The research article "Blockchain-Based Secure and Trusted Distributed International Trade Big Data Management System" explores the application of blockchain technology in international trade big data processing. It addresses the challenges of data security and reliability in the era of big data, emphasizing the potential value of data and the need for advanced encryption to ensure security. The study proposes a secure and trusted distributed network architecture and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

analyzes its performance through experimental results. It highlights the potential of blockchain technology to improve data utilization, reduce costs, and enhance security in international trade.

The document discusses the complex nature of international trade, emphasizing its fragmented and chaotic characteristics. It identifies the lack of modern information technology application as a key factor contributing to the inefficiency of international trade. The study introduces blockchain as a disruptive technology with the potential to revolutionize various aspects of international trade, such as data sharing, access control, and supply chain management. The advantages of blockchain technology, including improved data quality, transparency, and collaboration, are highlighted, positioning it as a solution to the challenges inherent in international trade.

The research also delves into the performance evaluation of the system, including tests on encryption and decryption, data upload and download performance, and throughput comparison between centralized and decentralized authorization managers. The experimental results demonstrate the superiority of the decentralized manager in processing a large amount of data, with peak throughput reaching about 450 pcs/sec, compared to the centralized manager's peak throughput of about 150 pcs/sec. The study also evaluates the system's performance in local area network and public network environments, demonstrating better performance in the local area network.

In conclusion, the research underscores the transformative potential of blockchain technology in the realm of international trade big data management. By addressing security concerns, improving data transparency, and enhancing collaboration, blockchain offers a promising solution to the challenges inherent in international trade. The comprehensive evaluation of the system's functionality, performance, and security further strengthens the research's validity and relevance in the context of modern trade practices.

Advantage: The research showcases how blockchain technology can revolutionize international trade big data management by enhancing security, reliability, and transparency. Through advanced encryption and decentralized authorization managers, blockchain offers improved data utilization, reduced costs, enhanced security, and increased collaboration in trade processes.

Disadvantage: Despite its benefits, implementing blockchain in international trade faces challenges such as performance variations in different network environments and barriers to widespread adoption, including interoperability issues, regulatory constraints, and industry adoption hurdles. These challenges may hinder seamless integration and require continuous refinement to ensure successful implementation.

2.10 Secured Multi-Layer Blockchain Framework for IoT Aggregate Verification

The study titled "Secured Multi-Layer Blockchain Framework for IoT Aggregate Verification" addresses the challenges in ensuring security, transparency, and traceability in the global supply chain, particularly focusing on large-scale production suppliers' upstream nodes. The proposed solution introduces a Multi-Layer Aggregate Verification (MLAV) system within a multi-layer IoT blockchain for Agriculture 4.0 supply chain management. The framework aims to enhance efficiency, effectiveness, and security compared to conventional blockchains. The study leverages aggregate verification to improve the security and efficiency of ID-based verification, reducing network traffic on the blockchain and transferring computing overhead to aggregator nodes.

The three-layer blockchain infrastructure involves IoT devices sensing and uploading data in Layer 1, smart contracts executing aggregate ID-based signature verification in Layer 2, and a batch converting and uploading data to Ethereum in Layer 3, thereby reducing gas fees. The study highlights the benefits of using a multi-layer IoT blockchain system, including reduced Ethereum gas fees, elimination of certificate management costs with ID-based Aggregate Verification, and improved traceability in the agricultural supply chain. The proposed framework provides a secure and efficient solution for Agriculture 4.0, aligning with the evolving technologies such as the Internet of Things, big data, artificial intelligence, cloud computing, and remote sensing.

Advantage: The study presents a novel Multi-Layer Aggregate Verification (MLAV) solution for IoT blockchain in Agriculture 4.0, addressing efficiency and security concerns in supply chain management. The proposed framework combines multiple layers and aggregate verification to enhance traceability and reduce costs, making it a valuable contribution to the field.

Disadvantage: While The study outlines the theoretical framework and benefits of the proposed solution, practical implementation details and real-world case studies could strengthen The study's applicability and provide insights into

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

its effectiveness in diverse scenarios. Incorporating empirical evidence or demonstrations would enhance the credibility of the proposed multi-layer blockchain framework.

2.11 Decentralized Attestation and Distribution of Information Using Blockchains and Multi-Protocol Storage

This paper titled "Decentralized Attestation and Distribution of Information Using Blockchains and Multi-Protocol Storage" delves into the integration of trusted computing technologies, particularly attestations, within blockchain networks to bolster their security, resilience, and survivability. It embarks on reviewing recent advancements in standard attestation architectures and evidence conveyance protocols, assessing their suitability and advantages within the context of blockchain networks.

Moreover, it confronts challenges arising from the evolving landscape of blockchain network deployments, such as the incorporation of virtualization technologies in cloud infrastructures. Through proposing a multi-protocol storage framework, which amalgamates established storage protocols like Git or IPFS with blockchain-based attestations, The study aims to fortify the verification of authenticity and timestamps for stored information. Preliminary implementation showcases technical feasibility and moderate performance on the Ethereum blockchain, setting the stage for further exploration across alternative blockchain platforms and potential integration with mechanisms for decentralized data processing and verification.

Advantage: Enhanced security and authenticity of stored information. By integrating blockchain-based attestations with existing storage protocols like Git or IPFS, the proposed multi-protocol storage framework ensures that stored data is verifiable and tamper-resistant. This enhances trust in the integrity of the information stored within the system.

Disadvantage: Potential scalability challenges. Implementing a multi-protocol storage framework may introduce complexities in managing and scaling the system, especially when dealing with large volumes of data or high transaction rates. Ensuring efficient performance and scalability while maintaining security could pose significant technical hurdles.

2.12 Safety Lies in Numbers - Proposing DDSP, a Decentralized Data Storage Protocol

The study titled "Safety Lies in Numbers - Proposing DDSP, a Decentralized Data Storage Protocol" presents a compelling solution to the shortcomings of centralized cloud storage systems. It advocates for the development of a decentralized data storage protocol, DDSP, which integrates blockchain technology and proof of retrievability to ensure data confidentiality, integrity, and availability. By distributing data across multiple storage providers and leveraging the decentralized nature of blockchain, DDSP offers a promising alternative that addresses concerns such as single points of failure and data security vulnerabilities inherent in centralized systems. The proposed protocol represents a significant step towards creating a more resilient and secure storage environment for both individuals and businesses.

Furthermore, the introduction underscores the pressing need for a paradigm shift in data storage approaches due to the vulnerabilities associated with centralized cloud services. It highlights the potential consequences of outages and insider attacks on data security and emphasizes the benefits of decentralized storage networks in mitigating these risks. By decentralizing computational resources and control structures, decentralized storage networks, such as the proposed DDSP, offer increased resilience and enable healthy competition among storage providers, ultimately leading to a more robust and cost-effective storage ecosystem.

Advantage: Enhanced security and authenticity of stored information. By integrating blockchain-based attestations with existing storage protocols like Git or IPFS, the proposed multi-protocol storage framework ensures that stored data is verifiable and tamper-resistant. This enhances trust in the integrity of the information stored within the system.

Disadvantage: Potential scalability challenges. Implementing a multi-protocol storage framework may introduce complexities in managing and scaling the system, especially when dealing with large volumes of data or high transaction rates. Ensuring efficient performance and scalability while maintaining security could pose significant technical hurdles.

2.13 Blockchain Enabled Metaheuristic Cluster Based Routing Model for Wireless Networks

The study proposes a Metaheuristic-based Clustering with Routing Protocol for Blockchain-enabled Wireless Sensor Networks (MCRP-BWSN) to address security challenges in Wireless Sensor Networks (WSN). This technique utilizes

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

blockchain technology to establish shared memory schemes and optimal route selection in clustered WSN. It employs the Chimp Optimization Algorithm (COA) for clustering and the Horse Optimization Algorithm (HOA) for routing, leveraging blockchain for shared memory among network nodes. Experimental analysis validates the effectiveness of MCRP-BWSN, demonstrating its superiority over existing techniques in terms of security and efficiency.

In summary, the MCRP-BWSN technique introduces a novel approach to achieve optimal route selection and security in WSN through blockchain-enabled metaheuristic clustering and routing. By utilizing COA and HOA along with blockchain technology, it addresses internal and external security threats while optimizing network performance. Experimental results confirm its effectiveness, paving the way for its application in various wireless network environments, including mobile adhoc networks and vehicular networks, thus contributing to the advancement of secure and efficient communication in IoT applications.

Advantage: The proposed MCRP-BWSN technique offers enhanced security for Wireless Sensor Networks (WSN) by leveraging blockchain technology. By utilizing blockchain for shared memory schemes and optimal route selection, it provides a robust defense against internal and external security threats, ensuring the integrity and authenticity of data transmitted within the network.

Disadvantage: Implementing blockchain technology in wireless sensor networks may introduce additional computational and energy overhead. The resource-constrained nature of sensor nodes could potentially be strained by the computational requirements of blockchain operations, leading to increased energy consumption and reduced network lifespan.

2.14 Blockchain Architecture Based on Decentralized PoW Algorithm

The study titled "Blockchain Architecture Based on Decentralised PoW Algorithm" presents a comparative review of various blockchain consensus algorithms, highlighting their strengths and weaknesses. It proposes a dissociated architecture for an efficient blockchain system that maintains security without compromising on efficiency. The proposed architecture leverages functionally specialized nodes to efficiently implement Proof of Work (PoW) consensus while minimizing computational expenses. The research aims to address the limitations of traditional PoW and other consensus algorithms by introducing the Dissociated-PoW algorithm.

Furthermore, The study contributes valuable insights into the strengths, vulnerabilities, and suitability of different consensus mechanisms for various blockchain applications. It proposes future work involving the development of a robust framework encompassing multiple consensus algorithms and emphasizing privacy safeguards across different blockchain architectures. Despite acknowledging certain limitations, such as the complexity of analyzing all possible combinations of blockchain networks and consensus algorithms, the research provides a foundation for advancing the field and shaping the future of decentralized systems.

Advantage: The proposed Dissociated-PoW algorithm efficiently implements Proof of Work (PoW) while minimizing computational expenses, making it more sustainable and scalable for diverse blockchain networks.

Disadvantage: Practical testing and validation of the Dissociated-PoW algorithm on various blockchain networks may face challenges in real-world implementation, requiring careful consideration to ensure effectiveness and security.

III. CONCLUSION

The study contributes by presenting a concise yet comprehensive technical architecture for a decentralized computational network. It emphasizes transparency, trustlessness, dynamic load balancing, incentive mechanisms, peer-to-peer consensus, smart contracts, and homomorphic encryption as crucial components of the proposed network. The exploration of these elements collectively aims to address the challenges associated with centralized computational systems.

This study provides a comprehensive overview of decentralization techniques and their application in building a resilient and efficient computational network. The focus of The study is on overcoming centralization challenges, including scalability issues and security concerns. It introduces key concepts such as dynamic load balancing, peer-to-peer consensus mechanisms, smart contracts, homomorphic encryption, and a novel tokenomics-based incentive structure.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

REFERENCES

[1]. Ihle, C., Trautwein, D., Schubotz, M., Meuschke, N., & Gipp, B. (2023). Incentive Mechanisms in Peer-to-Peer Networks — A Systematic Literature Review.

[2]. Naaz, R., & Kumar, A. (Year). Simulation of a Secure Approach of Data Communication on Peer-to-Peer Network Using Blockchain Technology on Ethereum.

[3]. Nazir, J., Iqbal, M. W., Alyas, T., Hamid, Dr, Saleem, M., Malik, S., & Tabassum, N. (2021). Load Balancing Framework for Cross-Region Tasks in Cloud Computing. Computers, Materials and Continua, 70, 1479–1490. https://doi.org/10.32604/cmc.2022.019344.

[4]. Shahzadi, K. (Year). Secure and Versatile Decentralized Ledger System Based on Blockchain for P2P Communication. International Journal of Computer Science and Telecommunications, 14(1), February 2023.

[5]. Carr, M. (2023). Blocktree: A Distributed Computing Environment. Retrieved from [Link](https://www.blocktree.systems/BlocktreeDce.pdf).

[6]. Ghosh, R., et al. (2023). DECENTRALIZED FILE STORING AND SHARING SYSTEM. Volume:05/Issue:05/May-2023, e-ISSN: 2582-5208.

[7]. Werth, J., Berenjestanaki, M. H., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma. ICEIS (1), 146-155.

[8]. Kabla, A., Anbar, M., Manickam, S., Ahmed, A., & Karuppayah, S. (2023). Monitoring Peer-to-Peer Botnets: Requirements, Challenges, and Future Works. Computers, Materials and Continua, 75, 3375-3398. https://doi.org/10.32604/cmc.2023.036587.

[9]. Sie, M. F., Wu, J., Harding, S. A., Lin, C. L., Wang, S. T., & Liao, S. W. (2022). Secured Multi-Layer Blockchain Framework for IoT Aggregate Verification. ASTES Journal, 7(3), 106-115. ISSN: 2415-6698.

[10]. Lian, G. (2022). Blockchain-Based Secure and Trusted Distributed International Trade Big Data Management System. Mobile Information Systems, 2022.

[11]. Zhang, X., Grannis, J., Baggili, I., & Beebe, N. L. (2019). Frameup: An incriminatory attack on storj: A peer to peer blockchain enabled distributed storage system. Digital Investigation, 29, 28-42. https://doi.org/10.1016/j.diin.2019.02.003.

[12]. Wilkinson, S., Lowry, J. (2014). Metadisk: Blockchain-Based Decentralized File Storage Application. Retrieved from [Link](https://www.storj.io/metadisk.pdf).

[13]. Wilkinson, S., Boshevski, T., Brandoff, J., Prestwich, J., Hall, G., Gerbes, P., ... (2016). A Peer-to-Peer Cloud Storage Network. Retrieved from [Link](https://www.storj.io/storjv2.pdf).

[14]. Vakilinia, I., Vakilinia, S., Badsha, S., Arslan, E., Sengupta, S. (2019). Pooling Approach for Task Allocation in the Blockchain Based Decentralized Storage Network. 2019 15th International Conference on Network and Service Management (CNSM), Halifax, NS, Canada. https://doi.org/10.23919/CNSM46954.2019.9012719.

[15]. Girgis, A. M., Ercetin, O., Nafie, M., & ElBatt, T. (2017). Decentralized coded caching in wireless networks: Trade-off between storage and latency. 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany. https://doi.org/10.1109/ISIT.2017.8006968.Salim DT, Singh MM, Keikhosrokiani P. A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. Heliyon. 2023 Jun 16.

[16]. Talib MA, Nasir Q, Nassif AB, Mokhamed T, Ahmed N, Mahfood B. APT beaconing detection: A systematic review. Computers & Security. 2022 Aug 21:102875.

[17]. Zou Q, Sun X, Liu P, Singhal A. An approach for detection of advanced persistent threat attacks. Computer. 2020 Dec 1;53(12):92-6.