International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

DIGITISED AND DECENTRALISED BLOCKCHAIN TECHNOLOGY

[1] Mrs.K.Indumathi,[2] P.Joshna,[3] J.Spandana,[4] R.Himabinbhu,[5] P.Usharani

[1]Assistant Professor,Department Of Computer Science And Engineering,Princeton Institute Of Engineering & Technology For Women Hyderabad.

[2,3,4,5] Students, Department Of Computer Science And Engineering,Princeton Institute Of Engineering & Technology For Women Hyderabad.

ABSTRACT

With ever-evolving technologies, the banking systems can update from their traditional methodologies to a digital, immutable, distributed ledger that can be implemented via Blockchain. Blockchain Technology is a distributed peer to peer linked structure which can solve the problem of maintaining and recording transactions in a banking system. Blockchain provides properties like transparency, robustness, auditability, and security. This paper aims at giving these functionalities in a distributed banking system using blockchain, which will be at par with the current methodologies. It will also focus on the limitations while implementing blockchain and future scope.

I.INTRODUCTION

Any banking system being the middleman between the transactions is vulnerable to threats like frauds, crashes, and cyber-attacks. Since almost all the banking systems are based on a centralized database, they are more prone to penetration attacks, which may compromise the confidential details of customers of the bank. As well as for the services provided by the bank, the customer has to pay the transactional overhead. On the other hand, the bank has to record and maintain all the transactional details for each customer, which is generally massive in

terms of data. Blockchain technology is the solution to these problems of the current traditional banking system. Blockchain technology originated when a white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” [1] was released in 2008 by Satoshi Nakamoto. This paper illustrates how to develop a peer-to-peer electronic cash system that allows online transactions between different parties without the involvement of the mediator. The World Economic Forum (WEF), in 2016 has suspected that blockchain technology will be able to transform financial services in the banking sector by creating a platform that connects consumers and producers directly [2]. The blockchain technology is a peer-to-peer distributed structure which could be used to overcome the issue in the traditional banking system. It is a collection of blocks that hold the encrypted transactional details sharing the same timestamp. The nodes of the network (miners) are responsible for linking the blocks to one another in chronological order, where each block contains the hash of the block created before in the chain. These hash values are the digital signature of each block and are dependent on two variables, first being the transactional details, and second is the hash value of the previous block. There are multiple hashing algorithms

like SHA256, RSA to achieve this. Even a minute change in any of the two variables will have a significant influence on the digital signature throughout the blockchain; thus overall, it provides a good security measure in a public ledger. Blockchain is a sequence of blocks distributed in a public ledger. Each block has a digital signature, which is in the form of hash code [3]. These hash codes are generated considering the parent block hash code and the set of transactions contained in the current block. The block is divided into two parts: Header and Body. As the name indicates, public blockchain is publicly available to everyone. In other words, public blockchain is open source in nature which means that anyone in the world who has access to the internet can participate in public blockchain. No consent of any person or organization is needed to participate in this blockchain. Any person can participate as a member, developer, community member or miner. Also, the code can be downloaded by anyone, and they can run the node on their local device. Basically, public blockchain is a permission less blockchain. All transactions done in public blockchain are fully transparent in nature. Everyone who is a member of public blockchain can view the transaction as it is transparent but at the same time it is anonymous. Bitcoin and Ethereum are the popular examples of public blockchain.

II.LITERATURE SURVEY

Blockchain technology has gained significant attention since its inception in 2008, when it was first proposed by an individual or group under the pseudonym Satoshi Nakamoto in the Bitcoin whitepaper. The fundamental innovation of blockchain lies in its decentralized nature, which allows data to be stored across a distributed network of nodes without the need for a central authority or intermediary. This decentralized structure ensures that all participants in the network have equal access to the same set of records, promoting transparency, security, and trust. Blockchain has since evolved to serve purposes far beyond cryptocurrency, and its applications now span a wide range of sectors, including supply chain management, finance, healthcare, intellectual property, and governance.

The key innovation of blockchain lies in its ability to guarantee the integrity of data stored on the blockchain. This is achieved through cryptographic techniques that ensure the immutability of records once they have been added to the blockchain. Each transaction is cryptographically signed, and the records are validated through a consensus mechanism before they are added to the chain. This process prevents unauthorized alterations to the data, thus promoting trust among participants. As blockchain technology continues to mature, researchers and practitioners have begun to explore various consensus mechanisms beyond the original proof-of-work (PoW) mechanism used by Bitcoin. Some examples include proof-of-stake (PoS), proof-of-authority (PoA), and delegated proof-of-stake (DPoS), each offering different benefits in terms of scalability, energy efficiency, and transaction speed. In the context of digitization, blockchain allows the secure digital storage and transmission of assets, contracts, and identities. This has significant implications for a variety of industries. For instance, in

supply chain management, blockchain enables the creation of a transparent, immutable ledger of product movements, allowing consumers and stakeholders to trace products back to their origin, ensuring authenticity, and reducing the risk of fraud. In healthcare, blockchain technology has been explored as a means of securely managing patient data, providing patients with control over their own health records while ensuring privacy and regulatory compliance. The integration of blockchain with the Internet of Things (IoT) is also being researched, as it provides an ideal solution to enhance the security and interoperability of connected devices, ensuring data integrity in real-time. Despite these promising applications, the adoption of blockchain technology faces several challenges. One of the primary concerns is scalability. As blockchain networks grow, the number of transactions processed by the system increases, leading to potential bottlenecks in performance. This issue has been particularly evident in platforms like Ethereum, where high transaction volumes can result in delayed processing times and increased transaction fees. Researchers have proposed various solutions, including sharding, off-chain transactions, and layer-two solutions like the Lightning Network, to address these scalability issues. Another challenge is the energy consumption associated with some consensus mechanisms, particularly proof-of-work. Mining operations for Bitcoin, for instance, require vast amounts of computational power, raising concerns about the environmental impact of blockchain networks. To mitigate these concerns, some newer blockchain systems have adopted more energy-efficient consensus mechanisms like PoS, which requires less computational work to validate transactions. Moreover, the lack of interoperability between different blockchain networks remains a significant challenge. Although blockchain allows for decentralized storage and transactions, it does not inherently.

III.METHODOLOGY

The methodology for implementing a digitized and decentralized blockchain system involves several critical phases, including system design, consensus mechanism selection, smart contract development, data encryption, scalability solutions, and privacy enhancements. The process begins with a thorough understanding of the problem domain and the specific industry or use case in which the blockchain solution will be deployed, whether that is healthcare, supply chain, or financial transactions. This domain-specific understanding is essential to determine the specific requirements of the system, including the types of data that need to be digitized, the privacy needs, transaction speed requirements, and potential for cross-chain interactions.

1. Requirement Analysis and System Design: The first step in the methodology is the collection and analysis of requirements. This phase involves conducting in-depth consultations with stakeholders to understand their needs and expectations for a decentralized system. Depending on the use case, this step might involve designing the blockchain's architecture, identifying the roles of various participants, and determining the types of assets and data that will be

managed on the blockchain. For example, in a supply chain scenario, the requirement analysis phase would involve identifying the types of products being tracked, determining the necessary attributes for each product (e.g., origin, condition, transport route), and understanding who needs access to the data and under what conditions.

2. Selection of Blockchain Platform and Consensus Mechanism: Once the requirements are clear, the next step is to select the appropriate blockchain platform and consensus mechanism. A significant challenge in blockchain implementation is choosing the right consensus algorithm that fits the specific requirements of the system. For instance, if the primary goal is to ensure low energy consumption and high transaction throughput, Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) might be more appropriate than the traditional Proof of Work (PoW) mechanism, which can be energy-intensive and slower in comparison. The consensus mechanism must ensure that all nodes on the network can reach an agreement on the state of the blockchain without the need for a central authority.

3. Smart Contract Development and Automation: The next phase is the development of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. Smart contracts are essential for automating transactions and ensuring that all parties involved in the blockchain network adhere to predefined rules. In this phase, developers write the code that dictates how assets will be transferred, how agreements will be enforced, and what actions will be triggered by specific events on the blockchain. Smart contracts can be used for a wide variety of applications such as automating supply chain processes (e.g., automatically triggering payment once goods are delivered) or managing patient records in healthcare, where predefined conditions trigger actions such as data sharing or access.

4. Data Encryption and Security Protocols: Since blockchain technology is widely used to store sensitive data, security is a critical aspect of the methodology. Blockchain data is encrypted to ensure the integrity of the stored information, preventing unauthorized access or tampering. The data on a blockchain is protected by cryptographic algorithms such as SHA-256 (in the case of Bitcoin), which produces a unique hash for each transaction. Additionally, digital signatures ensure that the sender's identity is verified, and the integrity of the data is preserved. If the system is dealing with sensitive personal data, like healthcare records, the use of advanced encryption techniques such as zero-knowledge proofs (ZKPs) can be employed to preserve privacy. ZKPs allow for the verification of transactions without revealing sensitive underlying data, enabling privacy-preserving blockchain applications.

5. Scalability Solutions: Scalability is a critical issue for blockchain systems, especially as they grow and handle increasing volumes of transactions. To address scalability challenges, the methodology integrates techniques such as sharding, off-chain transactions, and Layer-2 solutions. Sharding involves splitting the blockchain into smaller partitions (or "shards"), allowing

each shard to process transactions independently, thus improving overall throughput. Layer-2 solutions, such as the Lightning Network for Bitcoin or state channels for Ethereum, enable faster transactions off the main chain while preserving the security of the blockchain. These solutions allow the blockchain system to handle a larger number of transactions without compromising on performance.

IV.CONCLUSION

In conclusion, digitized and decentralized blockchain technology presents a transformative opportunity to revolutionize various sectors by enhancing security, transparency, and efficiency. While existing systems have made significant strides, challenges such as scalability, energy consumption, and interoperability still exist. The proposed system seeks to overcome these barriers by introducing more efficient consensus algorithms, improving cross-chain compatibility, and integrating advanced encryption techniques. The continued development and adoption of blockchain technology are likely to have far-reaching implications, including the democratization of data ownership, enhanced privacy, and the creation of more secure, decentralized networks. As the technology matures, it will be crucial to address regulatory concerns and ensure that blockchain solutions can integrate seamlessly with existing systems, paving the way for broader adoption in diverse industries.

V.REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

2.Buterin, V. (2013). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/

3. Wood, G. (2014). Ethereum: A Secure Decentralized Generalized Transaction Ledger. https://ethereum.github.io/yellowpaper/paper.pdf

4. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin.

5. Zohar, A., & Nehamiah, G. (2017). "Blockchain and the Future of Decentralized Economy". MIT Press.

6. Morrow, P. (2019). "Blockchain Beyond Bitcoin: How Blockchain is Revolutionizing

Supply Chain, Banking, and Identity Management." Blockchain Technology Insights, 45(3), 123-145.

7. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. NIST Special Publication 800-82.

8. Frizzo, T., & Salinas, A. (2021). "Blockchain: Applications and Limitations in Digital Transformation." Journal of Digital Innovation, 3(2), 88-103.

9. Vukolić, M. (2015). "The Blockchain Consensus Layer: Perspectives and Challenges." Future Generation Computer Systems, 47, 116-125.

10. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). "A Survey of Blockchain Technology: Evolution, Architecture, and Applications." Future Generation Computer Systems, 79, 28-46.