A Decentralized Approach to Online Transaction Security using Blockchain and Cryptographic Technology

Ashna Sachdeva[1], Saloni Ghule[2], Arihant Bhardwaj[3], Divij Kathuria[4]

School of Computer Science and Engineering

Vellore Institute of Technology, Chennai, India

ashna.sachdeva2021@vitstudent.ac.in, saloni.ghule2021@vitstudent.ac.in, arihant.bhardwaj2021@vitstudent.ac.in, divij.kathuria2021@vitstudent.ac.in

***Abstract*— This research explores how combining blockchain and advanced cryptography can significantly enhance online transaction security. By leveraging blockchain's distributed structure and innovative cryptographic techniques, this study addresses key challenges like scalability, consensus mechanisms, and privacy. It analyzes cryptographic methods capable of maintaining high transaction rates while ensuring data security, introducing approaches that protect data without obscuring it. Additionally, it enhances consensus algorithms to improve the capacity and efficiency of distributed systems. The findings provide recommendations for applying these technologies to strengthen online transaction frameworks, aiming to lay a secure foundation for the future of digital transactions.**

Keywords—Blockchain, SHA-256, online transaction, proof of work, cryptographic signature, data security, decentralized ledger.

I. INTRODUCTION

Blockchain technology, originally introduced with Bitcoin, has evolved beyond cryptocurrencies to become a powerful tool for ensuring data integrity, security, and transparency in various fields. Its decentralized nature, coupled with cryptographic principles, provides a robust foundation for secure online transactions. This paper delves into the application of blockchain for online transactions, highlighting the underlying mechanisms and their significance in modern financial systems.

Online transactions have become a fundamental part of the global economy, powering everything from e-commerce to digital banking. However, they are often plagued by challenges such as data breaches, fraud, and unauthorized modifications. Blockchain's immutable ledger offers a solution by creating a tamper-proof environment where every transaction is verified and recorded, reducing the potential for fraud and ensuring trustworthiness.

Implementing blockchain in online transactions enhances trust among users by eliminating the need for intermediaries. This decentralized verification process, based on cryptographic hashing and consensus algorithms, ensures that transactions are secure and immutable. As a result, blockchain can address prevalent issues like double-spending, a problem commonly faced in digital payment systems.

While various centralized systems use encryption to secure transactions, they often rely on trusted third parties for verification. This centralization poses a risk, as it creates a single point of failure and may be susceptible to hacking or manipulation. Blockchain eliminates this dependency, distributing transaction data across multiple nodes to ensure redundancy and resilience against attacks.

The proposed blockchain model for online transactions utilizes a Python-based implementation that follows a structured approach. It incorporates SHA-256 hashing for generating unique block identifiers and a proof-of-work (PoW) mechanism for maintaining consensus among participating nodes. The PoW system requires computational effort to add new blocks, ensuring that malicious actors cannot easily alter transaction records.

To authenticate transactions, cryptographic signatures are employed. This feature enables users to sign their transactions using private keys, which can later be verified with public keys to confirm the sender's identity. By leveraging asymmetric cryptography, the system ensures that only authorized transactions are processed, reinforcing data security and authenticity.

Blockchain's decentralized structure provides significant benefits over traditional centralized transaction systems. It is resistant to data tampering, enhances transparency, and allows traceability of all transactions within the network. Furthermore, once data is added to the blockchain, it is computationally impractical to alter, offering long-term data integrity and protection against fraud.

Despite its benefits, blockchain faces challenges such as scalability and energy consumption, particularly in PoW-based systems. Optimizing consensus algorithms and implementing hybrid approaches could address these limitations, balancing the need for security with practical performance. This paper discusses these challenges and explores solutions that make blockchain more adaptable for real-world applications.

The main objective of this paper is to outline the implementation of blockchain for online transactions using a secure Python-based framework. The following sections will detail the system architecture, hashing process, transaction verification mechanism, and block validation methods. We will also evaluate the system's performance and discuss its potential as an alternative for secure digital transactions.

II. Literature Review

Feng et al. [1] proposed a comprehensive survey, *"A Survey on Privacy Protection in Blockchain Systems"*, focusing on the critical issue of privacy in Blockchain beyond cryptocurrencies. The paper provides a clear definition of privacy, offering solutions for user and transaction confidentiality and identifying threats such as identity revelation and transaction exposure. It highlights countermeasures including Non-Interactive Zero-Knowledge (NIZK) proofs and homomorphic encryption, concluding with recommendations for advancing privacy-preserving solutions in Blockchain systems.

Wang et al. [2] examined Blockchain's application in *"Blockchain for Internet of Things (IoT)"*, addressing challenges related to data security and trust in IoT environments. The decentralized nature of Blockchain ensures data integrity and privacy, offering chain integrity through hash chains and anonymity with variable public keys. However, the scalability and network complexity challenges in IoT integration call for enhancements in consensus algorithms and data models.

Wen et al. [3] discussed *"Security and Privacy Protection Technologies in Securing Blockchain Applications"*, categorizing security concerns into data supervision, privacy protection, and data sharing. This paper explores current strategies and identifies potential improvements in privacy management systems and legal frameworks, emphasizing the ongoing need for research in Blockchain security solutions.

Meng et al. [4] introduced *"Enhancing the Security of Blockchain-Based Software Defined Networking through Trust-Based Traffic Fusion and Filtration"*. The BSDN Filter model combines Blockchain and SDN to secure data flow through dual-list filtration. This approach enhances data transfer and mitigates DoS attacks more effectively than previous methods like DistBlockNet, proving useful in distributed network environments.

Tripathi et al. [5] provided a *"A comprehensive review of Blockchain technology"*, tracing its evolution and highlighting its decentralized advantages over traditional systems. The study synthesized findings from 93 selected articles, showcasing Blockchain's pros and cons while noting ongoing security challenges. The review adhered to PRISMA 2020 guidelines for thoroughness and highlighted the technology's growing research relevance since 2015.

Venkatesan et al. [6] explored hybrid consensus algorithms in *"Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques"*, integrating ML for predictive attack detection and feature optimization. Hybrid models like DPoSW and PoCASBFT are proposed for increased security and scalability, recognizing real-world application challenges such as latency and resource constraints.

Ghazal et al. [7] developed a *"Private Blockchain-based encryption framework using computational intelligence approach"* for the IoMT. This framework secures patient data by storing records on a private Blockchain with controlled access for authorized personnel. The approach demonstrated high accuracy in training and validation phases, but faced challenges with device identification and permission authorization.

Samy et al. [8] focused on *"Enhancing the performance of the Blockchain consensus algorithm using multithreading technology"*, proposing an improvement to the Istanbul Byzantine Fault Tolerance algorithm. This modification increased transaction processing speed, addressing the limitations of energy-intensive consensus mechanisms like Proof-of-Work and enhancing network security and data consistency.

Kiran et al. [9] presented *"Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques"*, highlighting the integration of Blockchain with IoT and 5G networks. The paper underscores Blockchain's potential for secure data handling despite computational challenges with low-power IoT devices and 5G-related complexities, advocating for adaptive clustering techniques for better performance.

Tylor et al. [10] conducted *"A systematic literature review of Blockchain Cyber Security"*, which systematically examined how Blockchain technology is applied in cybersecurity. The study highlighted an increasing adoption of Blockchain solutions for addressing security concerns, especially within IoT systems. Despite recognizing the potential advantages, the study noted that research in this area is still relatively new, with most publications emerging after 2015. The authors suggest that future research should delve into practical implementations and evaluate the drawbacks to fully harness Blockchain's cybersecurity potential.

Taherdoost et al. [11] explored *"Smart Contracts in Blockchain Technology: A Critical Review"*, providing a detailed examination of smart contracts within Blockchain. Their literature review encompassed studies from 2012 to 2022, revealing that research on smart contracts has grown significantly, particularly post-2018. The review identified the predominant role of computer science and engineering in the field and noted extensive studies on smart contract applications across various industries. The research also highlighted China's significant contribution to this domain but pointed out the scarcity of economic analyses, suggesting potential avenues for expanded research. This work underlines the transformative potential of smart contracts across industries.

Wylde et al. [12] discussed *"Cybersecurity, Data Privacy and Blockchain"*, addressing the challenges Blockchain faces in data security and privacy. While Blockchain and smart contracts provide robust solutions for secure data transfer, the study notes ongoing concerns regarding user privacy and legal protections. The paper emphasizes the need for regulatory measures and technological enhancements to maximize Blockchain's effectiveness in cybersecurity.

III. Proposed Model

The proposed model implements a Blockchain framework as its core infrastructure to secure online transactions. This Blockchain is composed of a series of blocks linked through cryptographic hashes, ensuring that data integrity is maintained across the chain. Each block holds an index, the hash of the previous block, a timestamp, and transaction data. The chain is initialized with a genesis block, which acts as the foundational block with a static hash.

The model allows users to create new transactions via a web interface. A Flask-based web application handles user requests, where users input transaction details such as the sender, recipient, and transaction amount. These details are processed and passed to the backend for further verification and Blockchain integration.

To ensure the authenticity and non-repudiation of each transaction, the model employs asymmetric cryptography for transaction signing. A private key is used to sign transaction data, creating a unique signature that confirms the sender's identity. This ensures that only authorized users can initiate transactions, adding an additional layer of security.

The private key is stored securely in a PEM file and loaded using cryptographic libraries. The code includes a function to load this private key, and error handling mechanisms ensure that if the key is not found or fails to load, an appropriate message is returned to the user. This helps prevent unauthorized access and maintains the confidentiality of the private key.

The private key signs the transaction data using the RSA encryption algorithm with PKCS1v15 padding and SHA-256 as the hashing function. This process generates a digital signature that is unique to the transaction. The signature is then attached to the transaction data to validate the transaction's integrity when added to the Blockchain.

The model includes a proof-of-work (PoW) algorithm to secure the Blockchain network. This consensus mechanism requires miners to solve complex mathematical problems by finding a nonce value that, when combined with the last block’s hash, produces a hash that meets the difficulty criteria (e.g., starting with a specific number of zeros). The nonce acts as proof that a certain amount of computational effort was expended to validate the block.

Once the transaction is signed and added to the pool of current transactions, the Blockchain model mines a new block. The mining process involves calculating the proof of work using the proof_of_work method, which loops until the correct nonce is found. When successful, a new block is created and added to the Blockchain, including the new transactions and the proof of work.

Each block in the chain has a defined structure consisting of an index, the hash of the previous block, a timestamp, the transaction data, and the block's own hash. The calculate_hash method ensures that each block’s content is hashed using the SHA-256 algorithm, making any alterations immediately detectable, thereby maintaining data integrity.

The model stores transaction signatures in hexadecimal format to facilitate easy verification. During verification, the public key associated with the sender can be used to check the digital signature against the original transaction data. This prevents tampering and confirms that the transaction was initiated by the rightful owner of the private key.

The web interface built with Flask provides user-friendly endpoints for transaction submission and transaction history. Users input transaction data through an HTML form that is submitted to the submit_transaction route. The web application processes the data, signs the transaction, adds it to the Blockchain, and redirects users to a confirmation page.

The model features a route transaction_history that displays all transactions stored in the Blockchain. This route iterates through each block and extracts transaction data, displaying them along with details like block index and timestamp. This transparency helps users trace and verify all transactions on the network.

The integration of asymmetric encryption, transaction signatures, and the proof-of-work consensus ensures robust security. The private key signing process guarantees transaction authenticity, while the PoW algorithm secures the Blockchain against tampering and attacks like double-spending. Additionally, the Blockchain’s immutable nature ensures that once a block is added, its contents cannot be altered without recalculating the proof for all subsequent blocks.

While the current model demonstrates secure transaction handling and Blockchain integration, future work could focus on optimizing the PoW algorithm to reduce energy consumption and latency. Adding features like a public key infrastructure (PKI) for decentralized key management and integrating more advanced consensus mechanisms such as Proof of Stake (PoS) or hybrid models can further enhance security and scalability.

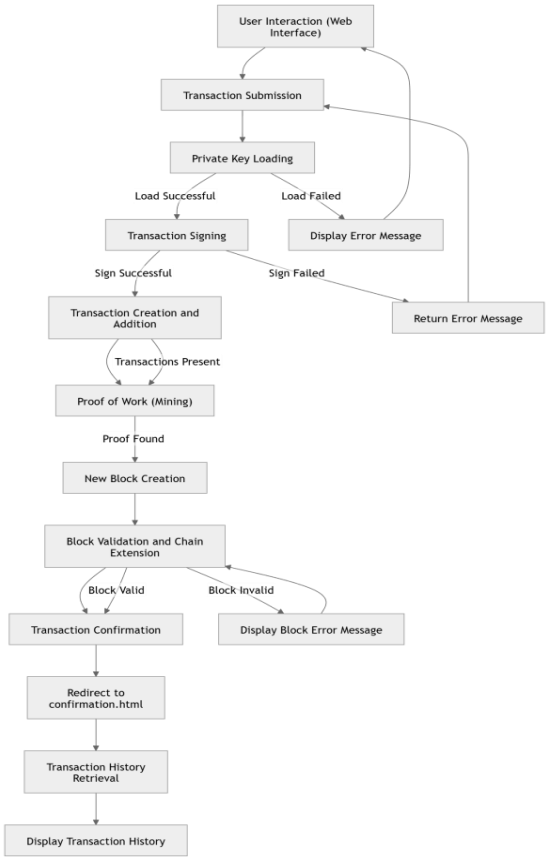

Figure 1: Proposed architecture

Figure 1 illustrates the proposed blockchain-based transaction system architecture designed for secure and transparent transactions. The system consists of a web interface, where users can submit transaction requests with details like sender, recipient, and amount. This interface is powered by Flask, which processes the submitted data through various backend functionalities

IV. Results

The proposed blockchain system begins with a user-friendly web interface that allows individuals to submit transaction details, such as the sender's information, recipient's details, and the amount to be transferred. The interface, powered by Flask, ensures seamless communication between the user and the underlying blockchain network. Upon submitting a transaction request, the system processes the data via the `submit_transaction` route, where the application extracts key information like the sender, recipient, and transaction amount, ensuring the request is ready for further processing.

For security and authenticity, the system requires the private key to sign the transaction. The `load_private_key()` function loads the private key from a PEM file, which is crucial for the digital signing process. If the private key cannot be found or loaded properly, the system raises an error, preventing the transaction from proceeding and ensuring that no unauthorized access occurs. The private key is used with the `cryptography` library to sign the transaction data using RSA encryption and the SHA256 hashing algorithm, providing a unique and verifiable signature that proves the legitimacy of the transaction.

Once the transaction is signed, it is appended to the blockchain's list of current transactions. These transactions are stored temporarily until they are added to a block, ensuring that the blockchain can handle multiple transactions at once. With the signed transaction added, the system then proceeds to calculate the proof of work required to add the transaction to the blockchain. The `proof_of_work()` method ensures that the transaction adheres to the blockchain's security protocol by finding a valid nonce that meets the difficulty level set by the system.

The mining process, through proof of work, ensures that only validated transactions are added to the blockchain. Once the correct nonce is found, the system creates a new block that contains the transaction, as well as crucial metadata like the block’s index, the previous block’s hash, the timestamp, and the list of current transactions. This block is then added to the blockchain, extending the chain and maintaining the continuity of the ledger.

Blockchain validation follows the creation of a new block, where the system checks the block’s proof of work and hash values. If the block meets the necessary conditions, it is successfully validated and added to the blockchain. This step ensures that the integrity of the blockchain is preserved, as only legitimate blocks that adhere to the consensus rules are included in the chain. The newly added block is now an official part of the blockchain, making the transaction part of the immutable ledger.

Once the block is added, the user is directed to the confirmation page, where they are provided with feedback on the transaction. The confirmation page displays all relevant details, such as the sender’s information, recipient’s details, the amount transferred, and the transaction signature. This provides the user with assurance that their transaction has been securely recorded and confirmed within the blockchain system.

In addition to individual transactions, the blockchain system allows users to access their transaction history through the `transaction_history` route. This feature provides a comprehensive overview of all past transactions stored in the blockchain, displaying transaction details like sender and recipient information, the transferred amount, and the timestamp. The transaction history page enhances transparency, allowing users to track the status and integrity of their transactions.

The blockchain system operates with a fixed difficulty for the proof of work process, ensuring a balance between transaction security and system efficiency. By requiring miners to find a nonce that results in a hash with leading zeros, the system safeguards against unauthorized tampering and ensures that only validated blocks are added to the blockchain. This mechanism adds an additional layer of security, making the blockchain resistant to fraud and manipulation.

This approach leverages both cryptographic techniques and consensus algorithms to build a secure, decentralized system where transactions are permanently recorded and cannot be altered once added to the blockchain. The system's architecture also includes various safety mechanisms such as the digital signature and proof of work, which help to ensure that all transactions are authentic and properly validated before they are accepted into the blockchain.

In conclusion, the proposed blockchain-based system is designed to provide a secure, transparent, and immutable method for handling transactions. Through its combination of digital signatures, proof of work, and blockchain validation, the system ensures that every transaction is properly verified and recorded, protecting users from fraudulent activities and ensuring the integrity of the blockchain. The integration of a user-friendly web interface also ensures that users can easily interact with the system, submit transactions, and track their transaction history, making the entire process smooth and reliable.

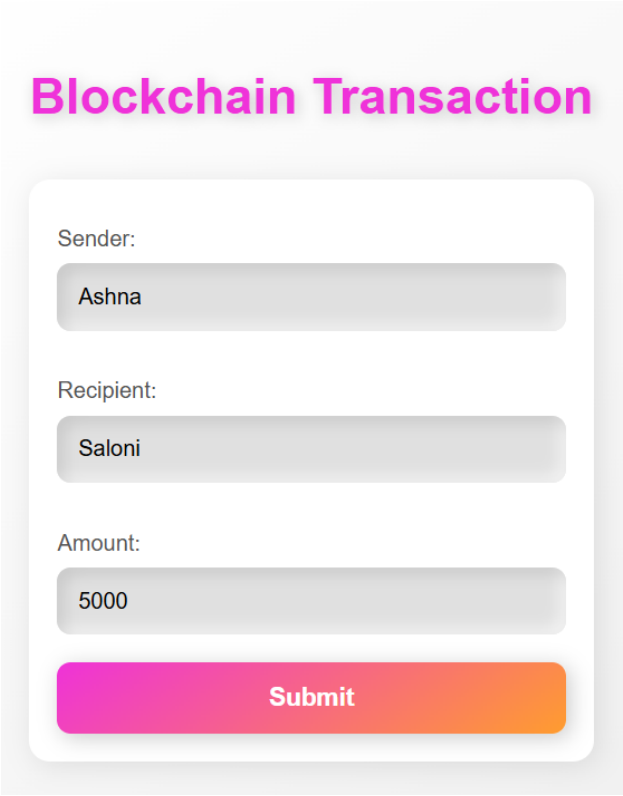

Figure 2: Transaction Input Form

Figure 2 This image displays a simple transaction input form with fields for the "Sender," "Recipient," "Amount and “Submit” button.

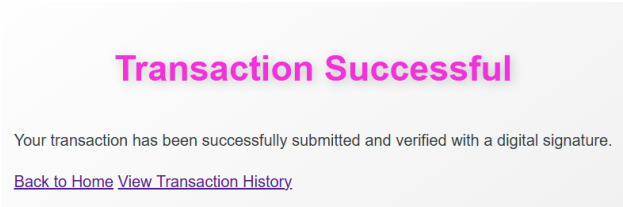

Figure 3: Transaction Success Message

Figure 3 shows a confirmation message indicating that a transaction has been completed successfully.

Figure 4: Transaction Log Confirmation

Figure 4 displays a console log message confirming the addition of a new transaction. The message states that a transaction from "Ashna" to "Saloni" for "5000 units" has been added. Below this, the "Transaction Signature" is shown, represented as a long alphanumeric string, likely a cryptographic hash, which serves as a unique identifier to verify the transaction's authenticity. The console output appears to be in a code or blockchain environment, emphasizing transparency and security by providing detailed transaction data, including the digital signature.

Figure 5 : Block Mining Confirmation Output

Figure 5 displays the console output which confirms the successful mining of the first block (Block Index 1) in a blockchain. This block contains a transaction which is secured by a unique digital signature to ensure authenticity. Key blockchain elements are displayed, including a "Proof" value of 42, which represents the proof-of-work needed to validate the block, and a "Previous Hash," linking it to the prior block and ensuring chain continuity. The block also has a unique "Hash" generated from its contents, providing tamper-proof security. This output encapsulates the essential features of blockchain technology, such as transaction validation, cryptographic linking, and data integrity through hashing.

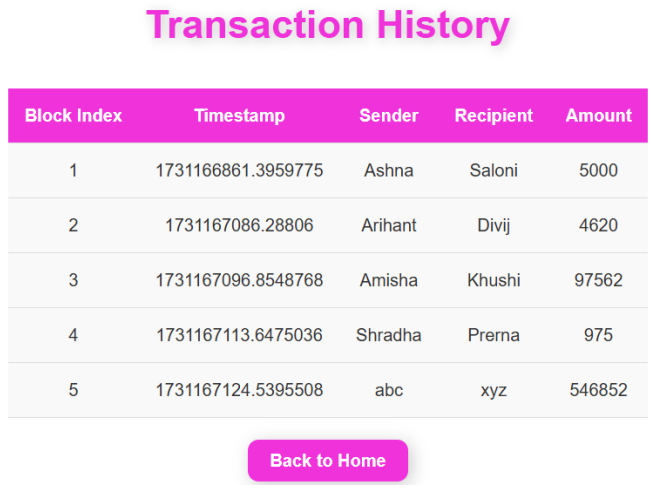

Figure 6: Blockchain Transaction History Table

Figure 6 displays a "Transaction History" table, showcasing details of blockchain transactions. Each row represents a transaction, with columns for Block Index (indicating the block number), Timestamp (showing the exact time of the transaction), Sender (the initiator of the transaction), Recipient (the receiver), and Amount (the value transferred).

V. Conclusion

In conclusion, the proposed blockchain-based transaction system effectively leverages advanced cryptographic techniques and the concept of proof of work to ensure the security, transparency, and integrity of transactions. By integrating a user-friendly web interface with robust blockchain architecture, the system provides a seamless experience for users to submit and track transactions. The incorporation of digital signatures ensures that each transaction is authentic and tamper-proof, providing

additional trust and security. Moreover, the blockchain's decentralized nature eliminates the need for intermediaries, making the transaction process more efficient and secure.

The successful implementation of this system demonstrates its potential as a reliable platform for secure transactions, with applications in various domains such as financial services and data integrity. Future improvements could include scalability enhancements and the integration of more advanced consensus mechanisms to handle a larger volume of transactions. However, the current system already showcases the key benefits of blockchain technology, offering a transparent, secure, and decentralized way to manage and verify transactions. As blockchain technology continues to evolve, it holds significant promise for revolutionizing various industries by providing more secure and efficient solutions.

VI. Future Works

Future work on this blockchain-based transaction system could focus on enhancing scalability to handle a larger number of transactions efficiently. As blockchain networks grow, the need for more efficient consensus algorithms becomes apparent. Implementing a scalable consensus mechanism like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) could significantly reduce transaction validation time and energy consumption, thus improving the overall system performance. These improvements would make the system more suitable for high-volume environments, such as global financial markets or decentralized applications that require fast and secure transaction processing.

Additionally, the integration of more advanced cryptographic techniques, such as zero-knowledge proofs (ZKPs), could further improve the privacy and security of the system. ZKPs would allow transactions to be verified without revealing sensitive data, thus ensuring privacy for users while maintaining the integrity and authenticity of transactions. This would be particularly useful in applications involving sensitive financial or personal data, providing users with a greater level of confidentiality without compromising the transparency and security of the blockchain.

Another area of potential future development is the user interface and experience. While the current system offers a basic web interface for submitting and tracking transactions, further enhancements could be made to make the platform more intuitive and accessible to a wider range of users. Implementing mobile-friendly designs, real-time transaction tracking, and advanced features like automated transaction categorization could improve usability, making the system more appealing to non-technical users. Moreover, incorporating features such as multi-signature support and integration with external payment systems would provide users with more flexibility and control over their transactions.

VII. References

[1] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 10.1016/j.jnca.2018.10.020.

[2] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, 10.1016/j.comcom.2019.01.006.

[3] Wen, B., Wang, Y., Ding, Y., Zheng, H., Qin, B., & Yang, C. (2023). Security and privacy protection technologies in securing blockchain applications. *Information Sciences*, 10.1016/j.ins.2023.119322.

[4] Meng, W., Li, W., & Zhou, J. (2020). Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. *Information Fusion*, 2020, 12. https://doi.org/10.1016/j.inffus.2020.12.006.

[5] Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Digital Applications in Aerospace, 2023*, 100344. https://doi.org/10.1016/j.dajour.2023.100344.

[6] Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports, 14*, 1149. https://doi.org/10.1038/s41598-024-51578-7.

[7] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Hamadi, H. A. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Engineering Intelligence Journal*, 2022, 06, https://doi.org/10.1016/j.eij.2022.06.007.

[8] Samy, H., Tammam, A., Fahmy, A., & Hasan, B. (2021). Enhancing the performance of the blockchain consensus algorithm using multithreading technology. *Alexandria Engineering Journal*, 2090-4479. https://doi.org/10.1016/j.asej.2021.01.019.

[9] Kiran, A.; Mathivanan, P.; Mahdal, M.; Sairam, K.; Chauhan, D.; Talasila, V. (2023). Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques. *Mathematics*, 11, 2073. https://doi.org/10.3390/math11092073

[10] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A systematic literature review of blockchain cybersecurity. *Digital Communications and Networks, 5*(3), 155-167. https://doi.org/10.1016/j.dcan.2019.01.005

[11] Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, 14, 117. https://doi.org/10.3390/info14020117

[12] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy, and blockchain: A review. *SN Computer Science, 3*(127). https://doi.org/10.1007/s42979-022-01020-4.