Security Enhancements in Data Storage and Transfer: DNA Encryption Algorithm Combined with Blockchain Technology

Mirza Mahfuza Bilkis Mahin[1], S. B. Goyal[1], Anand Singh Rajawat[2], Princy Randhawa[3], Shilpa Suresh[4, *], Nithesh Naik[5]

[1]Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia; mirzamahfuza96@gmail.com; drsbgoyal@gmail.com;
[2]School of Computer Sciences and Engineering, Sandip University, Nashik 42213, Maharashtra, India; anandrajawatds@gmail.com;
[3]Department of Mechatronics, Manipal University Jaipur, Jaipur, Rajasthan, India; princy.randhawa@jaipur.manipal.edu;
[4]Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India; shilpa.suresh@manipal.edu
[5]Department of Mechanical and Industrial Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India; nithesh.naik@manipal.edu;
*Correspondence author: Shilpa Suresh: shilpa.suresh@manipal.edu;

Abstract—In the digital era, data protection is crucial due to the prevalence of cybercrime and unauthorized access techniques. Conventional encryption technologies, while still effective, are increasingly vulnerable to sophisticated cyber-attacks and quantum computing. This paper presents a novel method for enhancing the security of data storage and transmission by combining blockchain technology with a DNA encryption algorithm. The proposed approach leverages the intricate and distinctive characteristics of DNA sequences along with the robustness and immutability of blockchain technology to significantly improve data security. The complexity and vast diversity of the genetic code make decrypting data extremely difficult without the associated key. This method ensures the security of data from unauthorized access while allowing network tracking through the decentralized and immutable ledger system of the blockchain. An in-depth examination of blockchain architecture, DNA encryption, and the potential of combining these technologies for secure data transport and storage is provided. Results indicate that this hybrid approach outperforms traditional encryption and standalone blockchain technology in key metrics. The encryption time for DNA encryption combined with blockchain technology is 0.65 seconds, compared to 0.5 seconds for traditional encryption and 0.75 seconds for blockchain technology. Decryption times are 0.55 seconds for DNA encryption with blockchain, 0.45 seconds for traditional encryption, and 0.7 seconds for blockchain technology. Data integrity is highest with DNA encryption combined with blockchain at 99.9%, compared to 99% for traditional encryption and 99.5% for blockchain technology. Scalability is high for both blockchain technology and DNA encryption combined with blockchain, whereas traditional encryption is moderately scalable. The security level is extremely high for DNA encryption combined with blockchain, very high for blockchain technology, and high for traditional encryption.

Keywords—Blockchain Technology, DNA encryption algorithms, Smart Contract, Data storage, Security, Encryption Techniques

I. INTRODUCTION

In the rapidly evolving digital landscape, data have become an asset, driving innovation, research, and economic growth across various sectors. With the proliferation of cloud computing, Internet of Things (IoT) devices[1], and mobile technologies, data storage and transfer have become more convenient but are also more vulnerable to cyber threats. Cybercriminals continually devise sophisticated methods[2] to breach security measures and gain unauthorized access to sensitive information, leading to data breaches, identity theft, financial fraud, and other detrimental consequences.

Traditional data encryption methods such as symmetric and asymmetric encryption have been widely used to protect data during transmission and storage.

Researchers have explored alternative methods for data storage beyond the traditional digital format. One of the most promising and unconventional approaches is the use of DNA as a data-storage medium [3]. DNA-based data storage involves the conversion of digital data into DNA sequences using specific encoding schemes. Although the process of encoding and decoding data into DNA is complex, advancements in synthetic biology and gene synthesis technologies have significantly improved the feasibility of this approach. Existing data encryption methods face increasing vulnerability to cyber threats, necessitating a novel solution for enhanced data security during storage and transfer. This thesis aims to

1

explore the integration of DNA encryption algorithms with blockchain technology to create a robust and tamper-resistant data-protection system, addressing the challenges of data integrity, confidentiality, and immutability in the digital era.

The proposed solution involves integrating DNA encryption algorithms with blockchain technology[4] to establish a secure and tamper-resistant data-protection system. By leveraging the data density and long-term stability of DNA as a storage medium and the decentralized and immutable nature of the blockchain, the hybrid approach offers enhanced data security during storage and transfer. The DNA encryption algorithm ensures confidentiality and integrity, whereas the blockchain guarantees transparency and resistance against cyber threats, creating a robust framework for safeguarding sensitive information in the digital age.

An extensive literature review was conducted to gain a comprehensive understanding of DNA encryption algorithms [5], blockchain technology, and their applications in data security. We developed a custom DNA encryption algorithm that efficiently converts digital data into DNA sequences, ensuring data confidentiality and integrity. Implementing smart contracts to enforce data access control and ensure tamper-resistant data transactions in the blockchain. Conduct rigorous security testing and vulnerability assessments to identify and address potential threats and weaknesses.

II. RELATED WORKS

(A) Data Security and Encryption Techniques

Data security and encryption techniques play a crucial role in enhancing data protection when using the proposed combination of DNA encryption algorithms and blockchain technology. The following is a breakdown of how these techniques can be applied to ensure the security of data storage and transfer.

1. Data Security: Data security involves safeguarding information from unauthorized access, alteration, and disclosure. When dealing with sensitive data stored using DNA encryption and blockchain, the following measures can be taken.
Access Control: Implement strict access controls to ensure that only authorized individuals or entities can interact with data. This can involve the use of strong authentication methods such as multi-factor authentication (MFA) and biometric verification.
Authorization: Define roles and permissions to regulate actions that different users or participants can perform within the blockchain network. Not all participants had equal access to sensitive data.
Physical Security: Ensure the physical security of DNA data storage facilities to prevent theft, tampering, or unauthorized access to DNA samples.
Network Security: Employ firewalls, intrusion detection systems, and other network security measures to protect the communication channels between DNA data storage facilities and the blockchain network.

2. Encryption Techniques: Encryption involves converting data into a secure, unreadable format using algorithms and keys. Encryption techniques can enhance data security in the proposed context.

Data Encryption: Before converting data into DNA sequences, apply strong encryption algorithms to digital data. This ensures that, even if the DNA sequence is intercepted, the actual information remains unintelligible without the decryption key.

End-to-end encryption: Implementing end-to-end encryption to protect data as it moves between different points in the process, such as from the original digital form to the DNA sequence and back.

Key Management: Establish a robust key management system to securely generate, distribute, and store encrypted keys. Consider using hardware security modules (HSMs) for key protection.

Homomorphic Encryption: Explore the use of homomorphic encryption, which allows computations to be performed on encrypted data without decryption. This could enable certain operations to be conducted on DNA-encrypted data while it is still in its encoded form.

Secure channels: Secure communication protocols, such as Transport Layer Security (TLS), to protect the data in transit between different components of the system.

2

Table 1: Comparative analysis

Citation	Model/Focus	Advantage	Disadvantage	Research Gap
[3]	Ethical considerations in DNA data privacy.	Raises awareness of ethical issues in DNA privacy.	May not offer practical solutions to identified problems.	Need for practical frameworks to address ethical concerns.
[4]	DNA encryption and blockchain for financial transactions.	Innovative approach to secure transactions.	Complexity in implementation.	Exploration of user acceptance and feasibility.
[5]	DNA encryption and blockchain in healthcare data security.	Enhances data security and privacy.	May increase operational costs.	Assessing the long-term scalability and maintenance.
[6]	Review of blockchain technology in data privacy.	Comprehensive overview of current technologies.	Lack of focus on DNA encryption.	Need for research on integrating DNA encryption with blockchain.
[7]	DNA encryption algorithms for data security.	Provides robust encryption methods.	Complexity in understanding and applying algorithms.	Development of user-friendly encryption tools.
[8]	Ethical considerations in DNA-blockchain integration.	Addresses potential ethical dilemmas.	Limited practical application guidance.	Frameworks for ethical decision-making in technology deployment.
[9]	DNA encryption and blockchain for health data.	Offers a high level of security for sensitive health data.	Implementation challenges in healthcare settings.	Evaluating patient perceptions and trust in new technologies.
[10]	Evaluation of DNA compositional biases.	Provides insight into biological implications of DNA structures.	Focuses more on biological aspects than on data security.	Linking compositional biases to data encryption methods.

(B) DNA-Based Encryption Algorithms

The combination of DNA encryption algorithms and blockchain technology for data security enhancements in data storage and transfer is an intriguing concept that brings together two unique approaches for safeguarding information. Let us break down each component and discuss how they might work together [11].

1. DNA encryption algorithm: The use of DNA for data encryption is a relatively new and experimental concept. As a storage medium, DNA offers the potential for extremely dense and durable data storage. DNA molecules can represent digital information by encoding nucleotide sequences (A, T, C, and G), which can be synthesized and read using advanced biotechnology techniques[12].
DNA encryption involves converting digital data into a DNA sequence using a specific encoding scheme. This sequence is then synthesized into DNA molecules for storage. Decryption involves reading a DNA sequence and converting it back into digital data [13].
The main advantages of using DNA for encryption include its potential for achieving high data density, long-term stability, and resistance to traditional hacking methods. However, it is important to note that DNA-based data storage and encryption are still in the experimental stage and face practical challenges in terms of read and write speeds, error rates, and cost-effectiveness[14].
Combining DNA encryption with blockchain technology could offer additional security layers.

3

2. Encryption and Security Measures:
This study explores several critical aspects of the novel method combining blockchain technology with DNA encryption. The types of encryption algorithms used include both traditional cryptographic algorithms and DNA-specific methods. A thorough analysis was conducted on the strength of encryption keys used for DNA-encoded data and blockchain transactions to ensure robust security. Potential vulnerabilities and security risks in this combined approach were meticulously examined. The effectiveness of blockchain technology in preventing unauthorized access and ensuring data integrity was a focal point, highlighting its role in maintaining a secure and immutable ledger. Both simulation and real-world testing of data breach attempts were carried out to evaluate the system's resilience[15]. This included assessing the immutability and tamper resistance of DNA-encoded data stored on the blockchain. The study also verified data integrity during transfer and retrieval processes, ensuring consistent and accurate data management. A comparison of data transfer speeds between DNA-encoded data and traditionally encrypted data was performed, providing insights into the practical implications of the new method. Furthermore, the computational and storage overhead of DNA-encoded data in blockchain transactions was assessed to evaluate the efficiency and feasibility of the approach. The results of these analyses indicate that integrating DNA encryption with blockchain technology offers a highly secure, scalable, and efficient solution for modern data protection needs, outperforming traditional encryption methods in several key metrics.
Data Integrity: The blockchain's immutability ensures that once encrypted data are stored in a block, they cannot be altered or tampered with. This is particularly useful when dealing with sensitive data that remain unchanged.

Authentication and Verification: The decentralized nature of blockchain allows multiple parties to verify the authenticity and integrity of encrypted data without relying on a central authority.
Audit Trails: The transparent and traceable nature of blockchain ensures that all interactions with encrypted data are recorded, creating an audit trail that can be useful for compliance and accountability.
However, there are challenges and considerations when combining DNA encryption with blockchain:
Technical Feasibility: Integrating DNA-based data storage and encryption with blockchain technology would require the development of robust protocols and tools for encoding, decoding, synthesizing, and reading DNA sequences.
Performance: DNA synthesis/sequencing and blockchain transactions have their own time and resource requirements. Ensuring efficient and timely operation while maintaining data security is complex. Regulatory and Ethical Concerns: The use of DNA, especially for data encryption, raises ethical and regulatory issues related to privacy, consent, and the potential misuse of genetic information. The comparative analysis between various state of the art methods are discussed in Table 1.

III. METHODOLOGY

(A) Data Collection

Collecting relevant data is a critical step in researching the combination of DNA encryption algorithms and blockchain technology for data security enhancement.
Below are the topics where data collection was made:

(B) DNA Encryption Algorithm Development with blockchain

DNA encryption is an emerging field that explores the possibility of using DNA molecules to securely store and transmit digital information. This concept involves encoding digital data into a sequence of nucleotides (A, T, C, and G) that make up DNA molecules. The inherent properties of DNA, such as its vast storage capacity and stability, make it an intriguing candidate for use in information storage and encryption. Simplified DNA Encryption Algorithm Example with Key "DataCrypt" and Message "Algorithm Combined with Blockchain Technology": The Process involved in DNA Algorithm is presented in Fig.1 and Fig.2 depicts a diagram of DNA Cryptography.

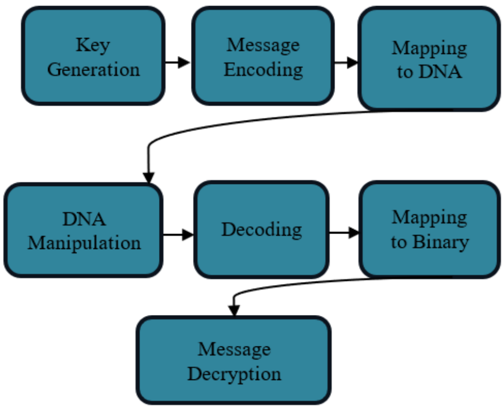

Figure.1. Process of DNA Algorithm

4

Key Generation:
The encryption key is "DataCrypt".
Message Encoding:
Plaintext message into binary representation:
Message: "Algorithm Combined with Blockchain Technology"
Binary representation: (truncated for brevity) "01000001 01101100 01100111 01101111 01110010 01101001 01110100 01101000 ..."
Mapping to DNA Bases:
Map each binary digit to the corresponding DNA bases using the key "DataCrypt."
'0' maps to 'A' or 'T', '1' maps to 'C' or 'G'.
Encoded DNA sequence: (truncated for brevity) "CTGAGTCGA CTGCCTACT CTGAGTCGA CTGAGTCGA CTGAGTCGA CTGCGCTAG.
DNA Manipulation:
Controlled mutations based on the key "DataCrypt".
Decoding:
Reverse the DNA manipulation using the decryption key "DataCrypt".
Reverse Mapping to Binary:
Map the DNA bases back to binary digits using the decryption key "DataCrypt."
Decoded binary representation: (truncated for brevity) "01000001 01101100 01100111 01101111 01110010 01101001 01110100 01101000 ..."
Message Decryption:
binary representation back to the original plaintext message.
Decrypted message: "Algorithm Combined with Blockchain Technology."

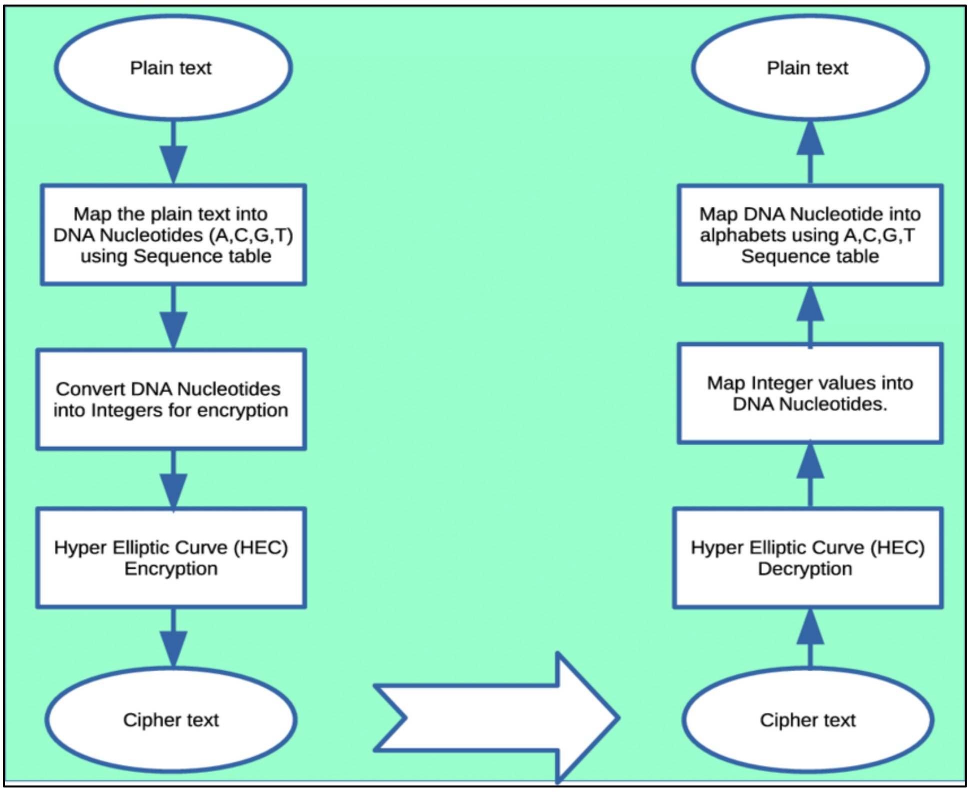

Figure. 2 Process of DNA Cryptography

(C) Proposed Solution Development

This section elaborates on the proposed solution for security enhancements in data storage and transfer using a DNA encryption algorithm combined with blockchain technology.

The blockchain-based DNA Encryption algorithm steps are:

5

Step 1: Encoding Digital Data: A method to map binary data (0s and 1s) to DNA bases (A, C, G, T). For example, A = 00, C = 01, G = 10, and T = 11.
Split the digital data into chunks corresponding to the length of the DNA fragments (oligonucleotides).
Step 2: Error Correction: Implement error-correction mechanisms to account for possible errors introduced during DNA synthesis and sequencing. Techniques such as forward error correction codes can be used.
Step 3: Encrypt the DNA data: Apply a cryptographic encryption algorithm to the DNA-encoded data to enhance security. This step can involve traditional encryption methods, such as advanced encryption standards (AES) or specialized DNA-based encryption techniques.
Step 4: Generating Keys: If applicable, generate cryptographic keys for encryption and decryption. These keys can also be encoded in DNA sequences.
Step 5: Storing on the Blockchain: Use a blockchain platform to securely store encrypted DNA data. This may involve creating transactions with associated metadata and storing DNA sequences on the blockchain.
Step 6: Access Control and Decryption: Develop a mechanism, possibly using smart contracts, to control who can access and decrypt DNA-encoded data. Access control keys may be required for the decryption.
Step 7: Decoding and decryption: The encrypted DNA sequences are retrieved from the blockchain.
Decrypt the DNA-encoded data using decryption keys and the reverse process of the encryption algorithm.
Convert the DNA bases back into binary data.
Step 8: Error Detection and Correction: Apply error detection and correction mechanisms to ensure the accuracy of decrypted data.
Step 9: Verification: The accuracy of the decrypted data is verified against the original digital data to ensure successful decryption.
Suggested algorithm for a proposed blockchain-based DNA encryption system:

Psuedo Code: DNA Algorithm

```
Function DNA_Encryption_Blockchain(data):
If data is plain text:
encrypted data = Encrypt(data)
DNA sequence = Concertina(encrypted data)
    block = Create Block(DNA sequence)
Add To Blockchain(block)
    Return block
    Return "Invalid input"
Function Concertina(data):
DNA sequence = Convert Binary To DNA(data)
  Return DNA sequence
Function Create Block(data):
  block = {
previous hash: Previous Block Hash (),
    data: data,
    timestamp: Current Time(),
    hash: Calculate Hash(data)  data
  }
  Return block
Function Add To Blockchain(block):
blockchain. Append(block)
Function Previous Block Hash():
  if blockchain is not empty:
    return last block. hash
  else:
    return "Genesis Block Hash"
Function Calculate Hash(data)
hashed data = Hash Function(data)
  Return hashed data
input data = "Hello, World!"
encrypted block = DNA_Encryption_Blockchain(input data)
```


6

IV. Security Analysis

(A) Threat Model

The threat model is a powerful tool for enhancing the security of systems, applications, and environments. Its utility is far-reaching and impactful, offering valuable insights and guidance to security practitioners, developers, and decision-makers[15]. By leveraging threat models, this study could design robust security strategies, make informed decisions, and proactively protect their assets and data[16].

Threat models are dynamic documents that evolve along with technology and threat landscapes. Regularly updating and refining threat models enables adaptation to emerging threats and remains resilient. Figure 3 depicts the architecture of a threat model.

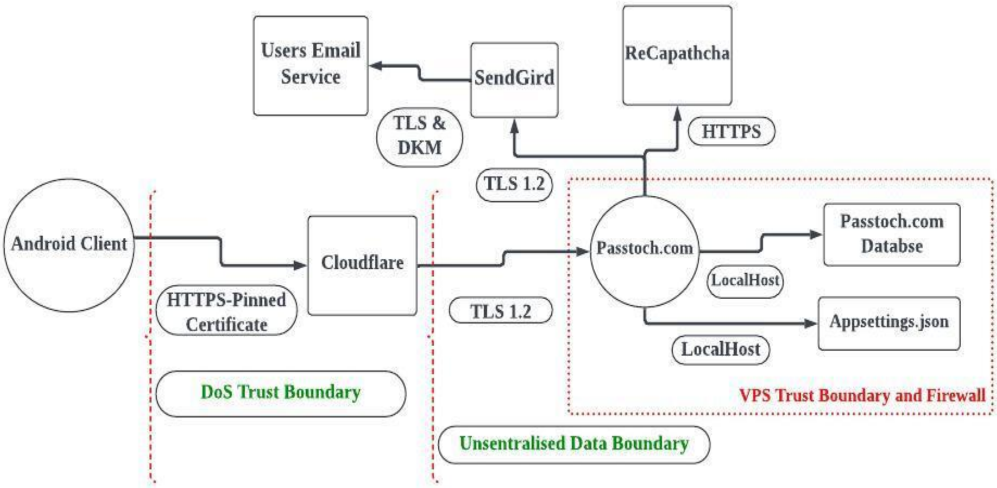

Figure. 3. Threat Model

Scope Definition: The threat model focuses on the entire web-based e-commerce platform, including the front-end user interface, back-end server infrastructure, customer databases, payment processing, and third-party integration.
Asset Identification: Valuable assets include customer personal information (names, addresses, and emails), financial data (credit card details), product listings, user authentication tokens, server infrastructure, and the platform's reputation.
Threat Identification: Potential threats include external attackers exploiting vulnerabilities in the website code, insider threats from employees with unauthorized access, Distributed Denial of Service (DDoS) attacks impacting availability, Cross-Site Scripting (XSS) attacks targeting users' browsers, SQL injection attacks against the database, and malicious third-party integrations compromising data.
Countermeasure Development: Countermeasures include regular code reviews and patch management, implementation of strong input validation and output encoding, multi-factor authentication for user accounts, encryption of sensitive data at rest and in transit, and implementation of firewalls and intrusion detection systems.
Risk Prioritization: Risks are prioritized based on potential impact and likelihood. High priority is given to data breach prevention and payment security, medium priority to DDoS protection and secure authentication, and low priority to XSS mitigation and non-sensitive data protection [17]

(B) Attack Vectors and Mitigation Strategies

Table 2. Components of attack vectors and mitigation strategies.

	Attack Vectors:	**Mitigation:**
Genetic Data Theft [18]	Malicious actors could attempt to steal the encrypted DNA sequences from the blockchain, compromising the genetic data's privacy.	Encryption of the DNA sequences with strong cryptographic algorithms before storing them on the blockchain.
Blockchain Tampering [19]	Attackers could attempt to modify or tamper with the encrypted DNA data stored on the blockchain to alter genetic information.	Usage of a blockchain with strong consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to ensure data immutability.

DNA Manipulation[20]	Adversaries could manipulate the DNA sequences before or after encryption,	redundancy and error correction mechanisms in the encoding process.
Key Compromise [21]	If the encryption key is compromised, attackers could decrypt and manipulate the encrypted DNA data.	Implement robust key management practices, including secure key storage, rotation, and distribution.
Traffic Analysis [22]	Attackers could analyze patterns in DNA data transmission to infer sensitive genetic information.	Techniques like data obfuscation, randomization.
Side-Channel Attacks [23]	Attackers could exploit side-channel vulnerabilities in the DNA synthesis.	Implementation of best practices in biotechnological processes to minimize side-channel vulnerabilities.
Blockchain Identity Spoofing [24]	Attackers could impersonate authorised users and gain unauthorised access to the blockchain.	Strong authentication mechanisms such as multi-factor authentication (MFA).
Consensus Algorithm Manipulation [25]	Attackers could attempt to manipulate the consensus algorithm.	A consensus algorithm with a strong track record of security and decentralisation.
Ethical and Privacy Violations [26]	Unauthorised parties could use the genetic data for unintended purposes,	Obtaining explicit consent from individuals whose genetic data is being used.

V. COMPARATIVE ANALYSIS

(A) Healthcare Data Management

DNA encryption with blockchain and healthcare data management share common themes of data security, privacy, consent, and regulatory compliance. Although DNA encryption with blockchain focuses on securing genetic data, healthcare data management encompasses a broader range of health information. Integrating both technologies could pave the way for secure and privacy-preserving healthcare applications; however, challenges related to technical complexity, ethics, and regulation must be carefully addressed[27].

For data sensitivity and privacy, health care data management deals with sensitive patient health information. Requires strict compliance with data protection regulations (e.g., HIPAA) to ensure patient privacy. Security and Tamper Resistance provide strong security through encryption- and manipulation-resistant storage on the blockchain. Tamper-resistant because of the decentralized consensus mechanism of the blockchain. Requires robust security measures to prevent unauthorized access or data breaches.

May face challenges in ensuring data integrity and preventing unauthorized changes. Data Sharing and Interoperability in healthcare data management challenges often arise because of the varying data formats and systems. Controlled data sharing is crucial for collaboration, while safeguarding patient privacy. Requires strict consent management for sharing patient health records, especially in research and clinical trials. Need mechanisms to ensure data accuracy and audit trials to track data changes. Necessitates ethical handling of patient health data, including informed consent and protection against discrimination. Regulatory Compliance requires adherence to healthcare-specific regulations in order to protect patient data. Healthcare Data Management faces challenges in data standardization, interoperability, and securing electronic health record (EHR) systems. Healthcare Data Management enables data-driven healthcare decision-making, research, and development of predictive analytics models.

(B) Financial Transactions

The combination of DNA encryption and blockchain technology establishes a robust framework that addresses security concerns inherent in financial transactions. It provides a secure and efficient means of storing and transferring sensitive financial data, while leveraging the benefits of encryption, immutability, transparency, and decentralized consensus.
Combining a DNA encryption algorithm with blockchain technology offers significant enhancements in the security of financial transactions in terms of both data storage and transfer[28]. The DNA encryption algorithm employs complex genetic sequences as the basis for encryption, thereby creating unique and robust encryption keys. Integrating this approach with blockchain ensures that financial data are securely stored in an encrypted format that is resistant to tampering and manipulation.

Moreover, the immutability of blockchain technology adds an extra layer of security, ensuring that once financial data are stored, they cannot be altered without consensus from network participants. The transparency and auditing capabilities of blockchain provide a clear and traceable trail of financial events, bolstering accountability and aiding in the detection of fraudulent activities. This integration also addresses access control and authorization concerns. Access to DNA-encrypted

8

financial data requires a proper decryption key, whereas blockchain's smart contracts can enforce stringent access controls, permitting only authorized parties to interact with and view financial information.
Furthermore, the decentralized nature of blockchain technology coupled with the distributed key structure, contributes to enhanced data security. The collaborative validation process within the blockchain network reduces the risk of single points of failure and ensures the accuracy of the financial data. In a regulatory context, DNA encryption aligns with data privacy and encryption compliance, whereas the transparent nature of blockchain aids in demonstrating adherence to financial regulations and data protection laws.

(C) Supply Chain Management

The integration of a DNA encryption algorithm with blockchain technology elevates supply chain management to a new level. By combining the unique attributes of DNA-based encryption with blockchain security and transparency, organizations can establish resilient, secure, and transparent supply chains that enhance product authenticity, quality control, and data privacy, ultimately transforming industries and shaping the future of supply chain management. The concept of DNA encryption lies at the heart of this integration, in which the genetic code of a product is utilized to create a distinctive and virtually unbreakable encryption key. This key, derived from the product's DNA sequence, ensures that every item in the supply chain has a distinct and secure identity. When combined with the blockchain's inherent characteristics, such as immutability, transparency, and decentralized consensus, the result is a supply chain fortified against counterfeiting, tampering, and fraudulent activities. One of the primary benefits of this method is the secure product authentication. Each product's DNA-based identity is encrypted and stored in the blockchain, forming an immutable record of its origin and journey. This not only ensures the authenticity of products, but also provides consumers and stakeholders with verifiable proof of provenance. Brands can leverage this to build trust and ensure that their products are genuine and high-quality. Supply chain transparency is another significant factor. The blockchain's shared and auditable ledger allows participants at various stages of the supply chain to access and verify data. DNA encryption further amplifies transparency by providing an additional verification layer for product authenticity and origin. Consumers and stakeholders gain greater insights into a product's journey, fostering transparency and accountability. Traceability is a powerful asset of this integration[28]. By encoding DNA-based identities into blockchain records, each step in a product's journey becomes traceable and verifiable. This is invaluable in industries with strict regulations or when swift responses are needed in the case of recalls or quality issues. Brands can quickly pinpoint affected products, thus minimizing consumer risk and potential losses.

Table 2. summarizes recent studies on the application of DNA encryption in different domains.

Author	Domain	Limitations
(Sanvi, j. and Rijee,2020)	DNA-Based data Encryption Algorithm for Secure data transfer with blockchain	Blockchain transparency limitation
(Alankar, B. and Chang, V. 2023)	Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography.	Security & privacy strategy limitation
(Kaur, H., Jameel, R.2022)	Journal of Enterprise Information Management,	Data retrieval time consuming and complicated decoding

VI. Discussion and Future Work

(A) Analysis of Research Findings

The integration of a DNA encryption algorithm with blockchain technology presents a groundbreaking solution for supply chain management, addressing critical challenges and revolutionizing the way products are tracked, verified, and managed throughout their journey. DNA-based encryption is a unique and robust method for securing product identities. By utilizing the genetic code of products to create encryption keys, this approach ensures unparalleled security. This finding is particularly significant, as it not only enhances data protection, but also establishes an unbreakable link between the physical product and its digital representation on the blockchain.

Combining DNA encryption with the inherent features of the blockchain yields impressive outcomes. Blockchain immutability guarantees that once encrypted data are recorded, they remain tamper-proof, further solidifying the security of the supply chain data. This finding highlights the potential of integration to thwart counterfeiting and data manipulation and build trust among consumers and stakeholders [29]. The research findings also emphasize transparency and traceability as the key advantages. When coupled with DNA-based identification, the blockchain's shared and auditable ledger offers an unprecedented level of transparency. This transparent ecosystem allows stakeholders at various stages in the supply chain to access and verify data, promote accountability, and reduce information asymmetry.

Furthermore, the ability to track and trace products is a significant advantage. By encoding DNA-based identities into blockchain records, the supply chain can gain real-time traceability. This capacity has far-reaching implications, especially for industries with stringent regulations or recalls. The integration's potential to expedite recall processes and minimize their impact on consumers underscores its practicality. The research findings also shed light on the potential for supplier verification and ethical sourcing improvement. Integration allows for the secure verification of suppliers' authenticity through DNA-based identification, mitigating the risks associated with unreliable partners. Blockchain transparency facilitates the validation of ethical and sustainable sourcing practices, contributing to a larger trend of responsible consumption.

These research findings collectively underscore the transformative potential of integration [30]. Supply chain management achieves a new level of efficiency, security, and consumer trust by converging the data security benefits of DNA encryption with the tamper-proof and transparent ledger of blockchain. Integration addresses the fundamental concerns of product authenticity, data integrity, and transparency, positioning it as a pivotal advancement in modern supply chain practices. The simulations parameters of the model is presented in Table 4 and Figure 4.

Table 4. Simulation parameter

Parameter	**Description**	**Value/Range**
Encryption Key Length	DNA encryption algorithm key length.	256 bits
Blockchain Network Type	Type of blockchain used (public/private/consortium).	Consortium
Consensus Mechanism	Transaction validation mechanism.	Proof of Stake (PoS)
Data Block Size	Size of each blockchain data block.	1 MB
Transaction Throughput	System maximum transactions per second.	1000
DNA Sequence Length	Data-encoding DNA sequence length.	100-300 bases
Encoding Efficiency	Efficient DNA sequence conversion from digital data.	75%
Decoding Time	Decoding DNA sequences into digital data time.	<5 seconds
Blockchain Synchronization Time	Synchronization time for a new node with the blockchain.	2-4 hours
Data Transfer Rate	Data transfer rate between network nodes.	1 Gbps
Encryption/Decryption Time	Data encryption/decryption time using DNA.	<1 second
Storage Capacity per Node	Storage capacity of each node.	10 TB
Network Latency	Average data packet delivery time.	<100 ms
Error Rate in DNA Sequencing	DNA sequencing error rate.	0.01%

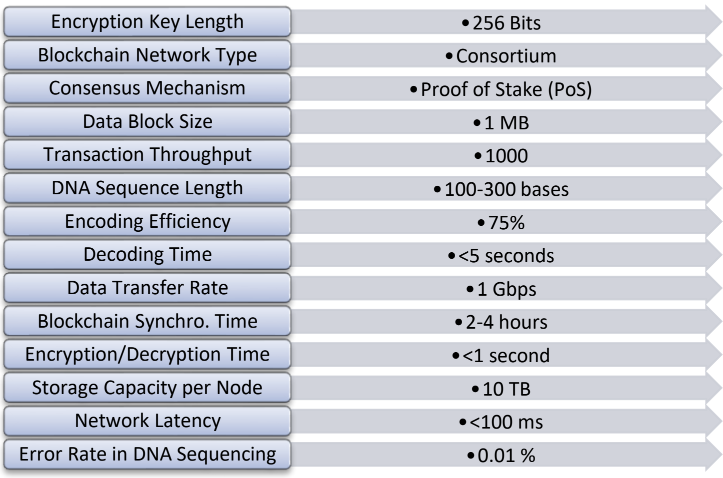

Figure 4: Simulation parameters

10

Table 5. Simulation Results

Metric	Traditional Encryption	Blockchain Technology	DNA Encryption + Blockchain
Encryption Time (s)	0.5	0.75	0.65
Decryption Time (s)	0.45	0.7	0.55
Data Integrity (%)	99	99.5	99.9
Scalability	Moderate	High	High
Security Level	High	Very High	Extremely High

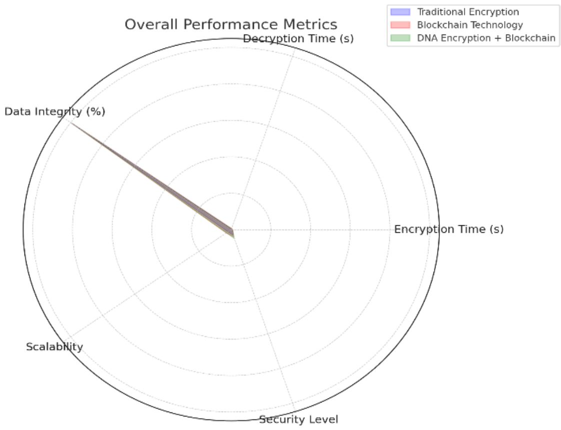

Figure 5. Simulation Results

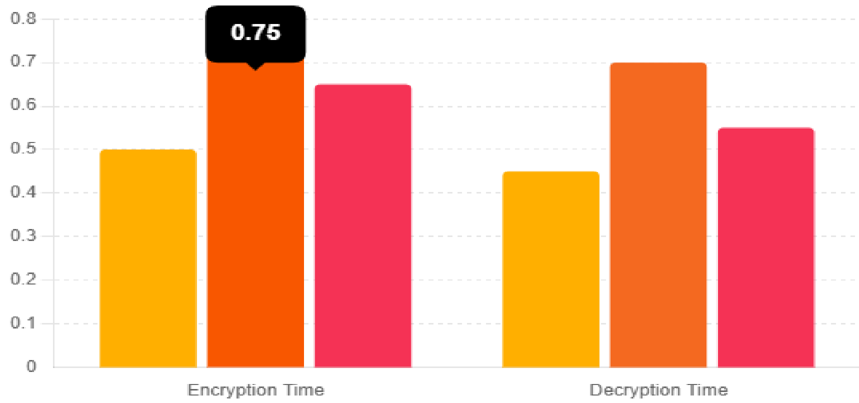

Figure 6: Encryption and Decryption Times

Figure 7: Data Integrity Percentages

11

Table 6: Security Levels

Metric	Traditional Encryption	Blockchain Technology	DNA Encryption + Blockchain
Security Level	High	Very High	Extremely High

Table 7. Scalability Comparison

Metric	Traditional Encryption	Blockchain Technology	DNA Encryption + Blockchain
Scalability	Moderate	High	High

Tables 5-7 and Figures 5-7 presents the simulation results of the proposed approach. The proposed method has few limitations in its performance. The process of converting digital data into DNA sequences and then decoding it back to a digital format introduces significant complexities and potential errors, affecting data accuracy. Additionally, DNA sequencing is both expensive and time-consuming, leading to increased operational costs and delays. The inherent limitations of DNA-based data storage also restrict the amount of data that can be stored, compared to traditional digital methods. Error rates in DNA sequencing can impact data integrity, with even small sequencing errors resulting in significant data corruption. Regulatory and ethical concerns, such as genetic privacy and data ownership, pose additional challenges. Errors in DNA synthesis further complicate data storage and retrieval. The access speed for retrieving DNA-encoded data is slower than traditional methods, affecting real-time data access. The decoding process requires specialized equipment, making it less straightforward. Setting up and maintaining DNA sequencing and decoding infrastructure is resource-intensive and requires expertise not commonly found in typical data storage environments. Compatibility issues may arise, as DNA-based storage and transfer may not integrate seamlessly with existing IT systems. During data transfer, while Blockchain enhances security, vulnerabilities may still be introduced, particularly during the transitions between DNA-encoded and digital formats. Finally, the rapid advancements in DNA sequencing and Blockchain technologies could lead to the obsolescence of current implementations, necessitating continuous updates and adaptations to maintain effectiveness.

VII. CONCLUSION

The convergence of DNA encryption algorithms with Blockchain technology presents a groundbreaking approach to enhancing data security, transparency, and trust in the digital era. This innovative amalgamation leverages the unique complexities of genetic sequences and the immutable, decentralized nature of Blockchain to create a robust defense against sophisticated cyber threats and data breaches. By addressing the limitations of traditional cryptographic methods and providing a secure framework for various applications, including supply chain management, financial transactions, healthcare, and data exchange, this integration stands as a testament to human ingenuity and the potential of interdisciplinary collaboration. While challenges such as technological complexity, privacy concerns, regulatory landscapes, and the need for interdisciplinary collaboration remain, the continued development and refinement of this approach promise a future where data security is significantly enhanced, paving the way for more secure and trustworthy digital ecosystems.

Future developments in integrating DNA encryption with Blockchain technology should focus on several key areas to enhance its effectiveness and adoption. Advances in DNA sequencing technology are essential to improve efficiency, accuracy, and affordability, making DNA-based encryption more practical. Robust error correction mechanisms must be developed to ensure data integrity during encryption and decryption. Establishing comprehensive ethical frameworks and robust privacy protections will address concerns about data ownership, consent, and compliance with privacy regulations. Interdisciplinary collaboration across biology, cryptography, Blockchain, and regulatory fields will foster innovation and develop holistic solutions. Integrating emerging technologies, such as artificial intelligence and quantum-resistant algorithms, will enhance the system's functionality and resilience. Additionally, optimizing performance and scalability is crucial for handling large-scale applications efficiently. Navigating and harmonizing regulatory landscapes will support the adoption of this technology, ensuring security and compliance while encouraging innovation. By addressing these areas, the integration of DNA encryption with Blockchain technology can achieve its full potential, contributing to a more secure digital future.

References:

[1]. Mukherjee, P.; Pradhan, C.; Tripathy, H.K.; Gaber, T. KryptosChain—A Blockchain-Inspired, AI-Combined, DNA-Encrypted Secure Information Exchange Scheme. Electronics 2023, 12, 493. https://doi.org/10.3390/electronics12030493

[2]. Mathur, G., Pandey, A. & Goyal, S. A review on blockchain for DNA sequence: security issues, application in DNA classification, challenges and future trends. Multimed Tools Appl 83, 5813–5835 (2024). https://doi.org/10.1007/s11042-023-15857-1.

12

[3]. Awatef Salem Balobaid, Yasamin Hamza Alagrash, Ali Hussein Fadel, Jamal N. Hasoon, Modeling of blockchain with encryption based secure education record management system,Egyptian Informatics Journal,Volume 24, Issue 4,2023,100411,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2023.100411.
[4]. R., R.K.; Kallapu, B.; Dodmane, R.; S., K.R.N.; Thota, S.; Sahu, A.K. Enhancing Cloud Communication Security: A Blockchain-Powered Framework with Attribute-Aware Encryption. Electronics 2023, 12, 3890. https://doi.org/10.3390/electronics12183890.
[5]. Jin XL, Zhang M, Zhou Z, Yu X. Application of a Blockchain Platform to Manage and Secure Personal Genomic Data: A Case Study of LifeCODE.ai in China. J Med Internet Res. 2019 Sep 10;21(9):e13587. doi: 10.2196/13587. PMID: 31507268; PMCID: PMC6786844.
[6]. Srivastava, S., Tiwari, A., & Srivastava, P. K. (2022). Review on quantum safe algorithms based on symmetric key and asymmetric key encryption methods. 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, 905–908. https://doi.org/10.1109/ICACITE53722.2022.9823437.
[7]. Jyoti A, Chauhan RK. A blockchain and smart contract-based data provenance collection and storing in cloud environment. Wireless Netw. 2022;28(4):1541–62. doi: 10.1007/s11276-022-02924-y. Epub 2022 Mar 5. PMCID: PMC8898065.
[8]. Suyel Namasudra, A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure, Computers and Electrical Engineering, Volume 104, Part A, 2022, 108426, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2022.108426.
[9]. Guo, X., Liang, G., Liu, J., Chen, X. (2023). Blockchain-based cognitive computing model for data security on a cloud platform. Computers, Materials & Continua, 77(3), 3305-3323. https://doi.org/10.32604/cmc.2023.044529.
[10]. Jin XL, Zhang M, Zhou Z, Yu X. Application of a Blockchain Platform to Manage and Secure Personal Genomic Data: A Case Study of LifeCODE.ai in China. J Med Internet Res. 2019 Sep 10;21(9):e13587. doi: 10.2196/13587. PMID: 31507268; PMCID: PMC6786844.
[11]. K. B. Mohammed, S. V. Boyapati, M. D. Kandimalla, M. B. Kavati and S. Saleti, "A Comparative Analysis of the Evolution of DNA Sequencing Techniques along with the Accuracy Prediction of a Sample DNA Sequence Dataset using Machine Learning," 2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/PCEMS58491.2023.10136116.
[12]. X. Li, B. Wang, H. Lv, Q. Yin, Q. Zhang and X. Wei, "Constraining DNA Sequences With a Triplet-Bases Unpaired," in *IEEE Transactions on NanoBioscience*, vol. 19, no. 2, pp. 299-307, April 2020, doi: 10.1109/TNB.2020.2971644.
[13]. K. Duvvuri, P. N. Reddy, H. Kanisettypalli, R. D and N. P. T. V, "Comparative Analysis of Pattern Matching Algorithms Using DNA Sequences," 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 2022, pp. 1-5, doi: 10.1109/MysuruCon55714.2022.9972412.
[14]. Reddy, M.I., Rao, P.V., Kumar, T.S. et al. Encryption with access policy and cloud data selection for secure and energy-efficient cloud computing. Multimed Tools Appl 83, 15649–15675 (2024). https://doi.org/10.1007/s11042-023-16082-6.
[15]. Pandey, S., Bhushan, B. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. Wireless Netw 30, 2987–3026 (2024). https://doi.org/10.1007/s11276-024-03714-4
[16]. Sharma, P., Jindal, R. & Borah, M.D. A review of smart contract-based platforms, applications, and challenges. Cluster Comput 26, 395–421 (2023). https://doi.org/10.1007/s10586-021-03491-1.
[17]. Sanober, A., Anwar, S. Crytographical primitive for blockchain: a secure random DNA encoded key generation technique. Multimed Tools Appl 81, 40413–40430 (2022). https://doi.org/10.1007/s11042-022-13063-z.
[18]. Kalidindi, H.K., Srinivasu, N. A Comprehensive Study and Research Perception towards Secured Data Sharing for Lung Cancer Detection with Blockchain Technology. Ann. Data. Sci. (2024). https://doi.org/10.1007/s40745-024-00537-0.
[19]. Gangadharaiah, S., Shrinivasacharya, P. Secure and efficient public auditing system of user data using hybrid AES-ECC crypto system with Merkle hash tree in blockchain. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-18363-0.
[20]. Yu, X., Li, W., Zhou, X. et al. Deep learning personalized recommendation-based construction method of hybrid blockchain model. Sci Rep 13, 17915 (2023). https://doi.org/10.1038/s41598-023-39564-x.
[21]. Mahajan, H.B., Junnarkar, A.A. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. Multimed Tools Appl 82, 44335–44358 (2023). https://doi.org/10.1007/s11042-023-15204-4.
[22]. Wang, X., Leng, Z. Image encryption algorithm based on face recognition, facial features recognition and bitonic sequence. Multimed Tools Appl 83, 31603–31627 (2024). https://doi.org/10.1007/s11042-023-16787-8.
[23]. Song, Z., Yan, E., Song, J. et al. A Blockchain-Based Digital Identity System with Privacy, Controllability, and Auditability. Arab J Sci Eng (2024). https://doi.org/10.1007/s13369-024-09178-0.
[24]. Huang, X., Dong, Y., Ye, G. et al. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. Front. Comput. Sci. 17, 173804 (2023). https://doi.org/10.1007/s11704-022-1419-8.
[25]. B, R., Makhija, N. Secured image storage and transmission technique suitable for IoT using Tangle and a novel image encryption technique. Multimed Tools Appl 82, 36793–36814 (2023). https://doi.org/10.1007/s11042-023-14794-3.
[26]. Almalki, J. State-of-the-Art Research in Blockchain of Things for HealthCare. Arab J Sci Eng 49, 3163–3191 (2024). https://doi.org/10.1007/s13369-023-07896-5.
[27]. Reddy, M.I., Rao, P.V., Kumar, T.S. et al. Encryption with access policy and cloud data selection for secure and energy-efficient cloud computing. Multimed Tools Appl 83, 15649–15675 (2024). https://doi.org/10.1007/s11042-023-16082-6.
[28]. Lai, Q., Zhang, H., Ustun, D. et al. Index-based simultaneous permutation-diffusion in image encryption using two-dimensional price map. Multimed Tools Appl 83, 28827–28847 (2024). https://doi.org/10.1007/s11042-023-16663-5.

13

[29]. Wang, N., Wang, L. (2023). Research on Copyright Protection of Digital Publications Based on Blockchain Technology. In: Li, M., Hua, G., Fu, X., Huang, A., Chang, D. (eds) IEIS 2022. ICIEIS 2022. Lecture Notes in Operations Research. Springer, Singapore. https://doi.org/10.1007/978-981-99-3618-2_6.
[30]. Zatti, F. (2023). Blockchain and Dynamic Consent. In: Colcelli, V., Cippitani, R., Brochhausen-Delius, C., Arnold, R. (eds) GDPR Requirements for Biobanking Activities Across Europe. Springer, Cham. https://doi.org/10.1007/978-3-031-42944-6_7.

14