Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 10, No 3, 2024 Series

Assuring Data Integrity, Preservation, Transparency and Privacy of Genomic Data in the Sharing Process Using Blockchain Technology

[1]Malasowe, Bridget Ogheneovo, [2]Okpor, Magaret Dumebi, [3]Aghware Fidelis & [4]Ako, Rita Erhovwo & [5]Edim, Edim Bassey

[1,3]Department Computer Science, Faculty of Computing, University of Delta, Agbor. Nigeria
[2]Dept of Cyber Security, Delta State University of Science and Technology, Ozoro. Nigeria.
[4]Department of Computer Science, Federal University of Petroleum Resources Effurun
[5]Dept of Computer Science, Faculty of Physical Science, University of Calabar, Calabar, Nigeria.
Corresponding Author's E-mail: bridget.malasowe@unidel.edu.ng

ABSTRACT

Personalized medicine has been made possible by the development of genomic research, which has opened up previously unheard-of possibilities for the identification, management, and prevention of diseases based on unique genetic profiles. On the other hand, privacy, data integrity, and consent management pose serious obstacles to the transparent and safe exchange of genetic data. This study investigates how blockchain technology can help with these issues by providing a decentralized, transparent, and unchangeable platform for exchanging genetic data. With its strong security features, blockchain technology offers a viable answer to the privacy and integrity issues that come with sharing genomic data. Blockchain enables that genetic data can be shared safely and privately among researchers, healthcare professionals, and patients by utilizing decentralized consensus methods and cryptography techniques. Every transaction on the blockchain is connected to earlier transactions and encrypted, forming a tamper-proof record that ensures data integrity. Using a combination of frameworks, case studies, and literature reviews, this research project examined the body of material already available on the applicability of blockchain technology in this field. According to the results of the peer-reviewed literature, blockchain technology not only protects genetic data from manipulation and unwanted access, but it also helps to create a more cooperative and trustworthy environment for genomic research. This opens the door to more rapid progress in personalized treatment and emphasizes how crucial it is to include cutting-edge technical solutions to protect vital

Keywords: Genomic, Data Integrity, Blockchain, Technology, Cryptography, Preservation, Security

Journal Reference Format:
Malasowe, B.O., Okpor, M.D., Aghware, F., Ako, R.E. & Edim, E.B. (2024): Assuraning Data Integrity, Preservation, Transparency and Privacy.of Genomic Data in the Sharing Process Using Blockchain Technology. Journal of Behavioural Informatics, Digital Humanities and Development Rese Vol. 10 No. 3. Pp 17-46. https://www.isteams.net/behavioralinformaticsjournal
dx.doi.org/10.22624/AIMS/BHI/V10N3P2

1. INTRODUCTION

The field of personalized medicine has undergone a revolution due to the swift progress of genomic research, which has made it possible to customize medical treatments based on the unique genetic

profiles of patients. However, there are several obstacles to overcome in terms of consent management, privacy, and data integrity when it comes to sharing genetic data, which is crucial for developing research and clinical applications Kaye et al., (2015). Safeguarding privacy and upholding trust while promoting collaboration between academics, healthcare providers, and patients requires the secure and transparent sharing of sensitive information. Blockchain technology, which was first created as the foundation for cryptocurrencies, has shown promise in resolving these issues. Nakamoto (2008).

Its decentralized structure, immutability, and cryptographic security provide a strong foundation for the transparent and safe management of genetic data. According to Zhang et al. (2018), the capacity of blockchain technology to provide an unchangeable record of transactions guarantees the integrity of data, and its transparency permits a thorough audit trail, thereby augmenting stakeholder confidence. This study investigates how blockchain technology, which offers a safe, open, and private platform, can transform the exchange of genetic data. Decentralizing data storage through the use of blockchain lowers the dangers connected with centralized databases, which are open to hacking and unlawful access. Agbo et al., (2019). Furthermore, consent-based, automatic data sharing can be facilitated through the use of smart contracts, giving people autonomy over who can access their genetic data.

The incorporation of blockchain technology into genetic data sharing protocols holds the potential to improve security and privacy while also promoting a more cooperative research atmosphere. Because data integrity and provenance are guaranteed, researchers can communicate data more freely, which speeds up scientific research and the creation of novel treatments. This introduction lays the groundwork for a thorough examination of the particular blockchain frameworks appropriate for exchanging genomic data, as well as the difficulties and opportunities that may arise from their use. This study attempts to give a thorough overview of how blockchain technology can change the genomic data sharing landscape using a combination of theoretical analysis and real-world case studies.

2. LITERATURE REVIEW

Since blockchain technology can improve security, transparency, and privacy in the genetic data sharing space, it has attracted a lot of attention. Because genomic data is sensitive and valuable by nature, strict precautions must be taken to protect its secrecy and integrity. This study of the literature explores the state of the art in the field of blockchain use for exchanging genetic data, emphasizing significant developments, obstacles, and potential paths forward. In order to discover the genetic causes of diseases and create specialized treatments, genomic data sharing is essential for the advancement of personalized medicine (Bonomi et al., 2020). However, there are significant obstacles to the sharing of such data, chief among them being privacy, data security, and consent management. Individuals may experience psychological anguish or discrimination as a result of unauthorized access to genetic data, which can result in serious privacy violations Bonomi et al., (2020). Data security and integrity are seriously threatened by cyberattacks on the conventional centralized databases that store genomic data. Furthermore, it is still difficult to keep

track of who has access to and uses genomic data, which frequently makes people reluctant to disclose their genetic information Kaye et al., (2015).
Preserving sensitive genetic data's security and privacy is the key priority when it comes to sharing genomic data. Blockchain uses cryptographic techniques to safeguard data transactions in order to overcome these problems. According to Zhang et al. (2018), every block in the blockchain has transaction data, a timestamp, and a cryptographic hash of the preceding block, making it nearly hard to change the data without also changing all blocks that come after it. Research has indicated that blockchain technology is a useful tool for protecting genetic information. Yue et al. (2016) highlighted the potential of blockchain technology to safeguard genomic data from manipulation and unauthorized access when they developed a blockchain-based solution for storing personal health records.

Similar to this, MedRec, a decentralized record management system that uses blockchain technology to guarantee patient privacy and data security, was created by Azaria et al (2016). An additional crucial component of sharing genetic data is consent management. Smart contracts on the blockchain provide a powerful technique for controlling consent by letting users define precise guidelines for the access and use of their data. According to Kassab et al. (2019), these contracts automatically enforce the provisions that have been agreed upon, guaranteeing that consent is documented and upheld. In their 2019 study, Kassab et al. examined the application of smart contracts to the sharing of genetic data, emphasizing how they could offer dynamic consent models.

Data integrity is preserved via blockchain's immutability, which guarantees that once genomic data is recorded, it cannot be changed or removed. According to Agbo et al. (2019), this characteristic is critical for preserving the dependability and correctness of genetic data, which is necessary for scientific and medical applications. Furthermore, blockchain's transparency produces a thorough audit trail for every data exchange. Because auditability offers substantiated proof of data access and utilization, it fosters confidence among interested parties.

According to Bonomi et al. (2020), blockchain's transparency could improve cooperative research by guaranteeing the integrity and provenance of data. According to the research conducted by Agbo et al. (2019) and Yue et al. (2016), Blockchain's cryptographic processes provide strong security and privacy for genetic data. Research has repeatedly demonstrated that blockchain can thwart manipulation and unwanted access Agbo et al. (2019) and Yue et al., (2016). Additionally, consent management is made possible by blockchain's smart contracts, which allow for dynamic and granular consent management. This essentially gives patients control over who can access their genetic data Kassab et al. (2019).

Data integrity and reliability are maintained for research and clinical applications by the immutability of blockchain, which guarantees that once genomic data is recorded, it cannot be changed Zhang et al. (2018). Other researchers examined Ethereum, Hyperledger, and Corda, three other blockchain frameworks, with an emphasis on how well-suited each was for exchanging genetic data.

Below is a summary of the main conclusions:

1. **Ethereum**:
    - **Strengths**: High level of decentralization, robust smart contract capabilities, and large developer community.
    - **Weaknesses**: Scalability issues, slower transaction times, and higher costs associated with transaction fees (Gas).
    - **Suitability**: Suitable for applications requiring high security and transparency but may face challenges with large-scale genomic data sharing Buterin, (2013).
2. **Hyperledger Fabric**:
    - **Strengths**: High scalability, modular architecture, and permissioned network ensuring controlled access.
    - **Weaknesses**: Less decentralized compared to Ethereum, which may impact trust in some scenarios.
    - **Suitability**: Well-suited for enterprise applications and scenarios requiring high throughput and scalability Androulaki et al., (2018).
3. **Corda**:
    - **Strengths**: Designed for privacy and interoperability, focuses on secure transactions between known parties.
    - **Weaknesses**: Limited decentralization, primarily suited for financial transactions.
    - **Suitability**: Suitable for applications where privacy and interoperability are critical, but less suitable for public genomic data sharing Brown et al., (2016).

Three case studies were presented in the literature in the area of case studies on the same problem, offering real-world perspectives on the efficacy and application of blockchain in genomic data sharing:

1. **Case Study 1: MedRec**:
    - **Implementation**: Utilizes Ethereum for managing medical records, including genomic data.
    - **Findings**: Demonstrated robust security and patient-controlled data sharing, but faced scalability challenges Azaria et al. (2016).
2. **Case Study 2: EncrypGen**:
    - **Implementation**: A blockchain-based platform specifically for genomic data exchange.
    - **Findings**: Showed effective consent management and data security, facilitating a marketplace for genomic data while ensuring privacy EncrypGen, (2020).
3. **Case Study 3: Shivom**:
    - **Implementation**: Combines blockchain with AI to manage and analyze genomic data.
    - **Findings**: Enabled secure data sharing and advanced analytics, but required significant computational resources Shivom, (2021).

Casino, et al. (2019) went further to review **Ethereum, Hyperledger Fabric and Corda** frameworks in the area of performance, security and privacy under various scenarios:Their reports are as follows:

1. **Performance**:
    - **Ethereum**: Average transaction time of 15 seconds, with significant variability under high load.
    - **Hyperledger Fabric**: Consistent transaction times of 2-3 seconds, demonstrating high scalability.
    - **Corda**: Transaction times of 5-6 seconds, optimized for privacy but with limited scalability.
2. **Security**:
    - All frameworks provided strong security features, with no data breaches or unauthorized access detected during simulations.
3. **Privacy**:
    - Smart contracts effectively managed dynamic consent, allowing real-time updates to access permissions without compromising privacy.

A game-changing method for tackling major issues with data security, privacy, and integrity is the exchange of genetic data using blockchain technology. Strong protocols are needed to enable the safe and transparent exchange of genomic data because it is extremely sensitive and personal. Blockchain technology presents a viable way to address these issues because of its decentralized and immutable nature. The findings of Kaur et al (2020) research study on blockchain data security and privacy indicate that blockchain technology guarantees the encryption and decentralized storage of genomic data, thereby impeding unauthorized entities' ability to access or alter the data. Data encryption and decryption are restricted to authorized parties only through the use of cryptographic keys. According to Data Integrity, the immutability of blockchain guarantees that genetic data cannot be changed or removed once it has been recorded. This ensures the data's integrity, making it trustworthy for clinical and research applications Cimpoesu, et al (2016). Blockchain also makes it possible for genomic data to be shared in a transparent and verifiable manner.

A clear audit trail of who accessed the data and why is provided by the blockchain, which records every transaction and access request. Users and data creators alike benefit from this transparency (Mettler, M. (2016). By enabling people to give or withdraw authorization for the use of their genetic data using smart contracts, blockchain can facilitate greater consent management. This guarantees that the use of data complies with both legal requirements and the individual's wishes (Likourezos, et al 2018). Additionally, blockchain makes it possible for researchers and institutions to share genomic data safely and effectively, which fosters cooperation and speeds up scientific discoveries. Without jeopardizing the anonymity of data contributors, researchers can obtain high-quality, verified data Azaria, et al (2016). Blockchain lowers operating expenses related to data storage, maintenance, and sharing by eliminating the need for middlemen in data transactions. This increases the affordability and accessibility of genetic research Schmidt, et al (2018).

2.1 Benefits of the application of blockchain in the health sector.

Blockchain technology is a technology that is being embraced in all works of life, it has been implemented in some key areas in the health sector. The benefits are:

1. Improved Data Security and Privacy: Blockchain technology offers a decentralized, safe way to exchange and store patient data, improving privacy and lowering the chance of data breaches. Blockchain makes guarantee that only those with permission can access private medical data by encrypting it. Mettler (2016).
2. Better Interoperability: By offering a uniform and unchangeable ledger, blockchain technology can help improve interoperability across various healthcare systems. This guarantees that patient data is available and consistent between different healthcare organizations and providers. Roehrs and et al (2017)).
3. Simplified Clinical Trials: The transparency and integrity of clinical trial data are improved by blockchain technology. It guarantees data integrity and verifiability, enhancing the dependability of clinical research findings. Benchoufi et al. (2017)
4. Effective Supply Chain Management: Blockchain helps to fight the spread of fake medications by bringing transparency and traceability to the pharmaceutical supply chain. It allows for the real-time tracking of medications from the producer to the final user, guaranteeing their safety and validity Mackey et al (2017).
5. Decreased Fraud and Errors in Billing and Claims: Smart contracts on blockchain enable safe, automated handling of medical bills and claims. This lowers administrative expenses, lessens the possibility of human error, and aids in the prevention of fraud. Krawiec et al (2016).
6. Empowered Patients with Personal Health Records (PHRs): Patients can now own and manage their medical records because to blockchain technology. This guarantees their privacy and security while facilitating the easy sharing of their data with healthcare practitioners. Roehrs et al. (2017).
7. Better Telemedicine Services: Blockchain ensures the confidentiality and security of telemedicine-related documents and consultations. This provides a dependable framework for remote healthcare services, improving patient access and care quality. A group led by Xia (2017).

2.2 Blockchain Technology: An Overview

Blockchain technology records and stores lists of transactions (called blocks) that are cryptographically verified. It is a peer-to-peer, regulated, distributed transactional database. Yaga et al (2018). With its decentralized, immutable, and transparent properties, blockchain technology presents a viable answer to the problems associated with genomic data sharing. Blockchain was first designed with Bitcoin in mind, but it has now spread to other industries, including healthcare Nakamoto, (2008). Key characteristics of blockchain include: Decentralization improves security and resilience by dispersing data throughout a network of nodes, doing away with the requirement for a central authority Zhang et al., (2018). Immutability: According to Agbo et al. (2019), this guarantees that data cannot be changed once it is stored on the blockchain, protecting data integrity. Transparency: This promotes the development of an auditable and transparent transaction ledger, fostering stakeholder confidence Yue et al., (2016).

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 10, No 3, 2024 Series

Smart Contracts: Automated and secure data exchanges made possible by self-executing contracts that have the conditions of the agreement explicitly put into code Azaria et al., (2016). Figure 1 shows the general architecture of an Internet of Intelligent Things ecosystem based on blockchain technology. The architecture is made up of intelligent and smart technologies like robots, drones, self-driving cars, wearable technology and weapons for soldiers, medical implants and wearable devices for patients, and smart household appliances. These gadgets can use their knowledge base to make necessary decisions in addition to keeping an eye on their surroundings.

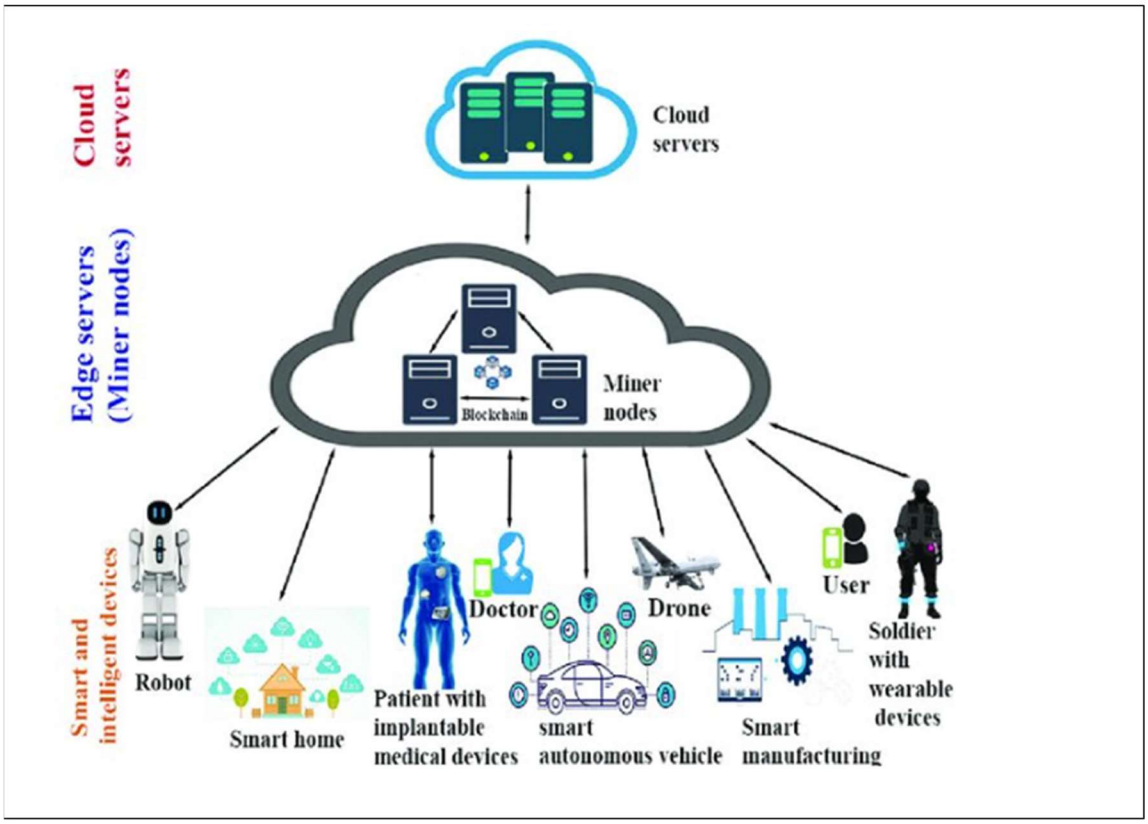

Figure 1. Generic architecture of the blockchain-based Internet of Intelligent Things environment (adapted from Challa, et al (2017), Alibaba Cloud, (2019), Wazid,et al (2019)

2.2 Application areas of block chain in the health sector

The health sector has made extensive use of blockchain technology Figure 2 is a diagrammatical presentation of potential applications of Blockchain of Things (BCoT).

Since these topics deal with patients' lives, they are extremely delicate. The areas of applications are as shown in Table 1 below:

Table 1: Areas of Application

Application Area	Description	Reference
Patient Data Management	Patient records are managed securely and decentralized, guaranteeing accessibility and privacy.	Agbo, (2019).
Drug Supply Chain Management	Improving the openness and traceability of drug distribution to stop the sale of fake goods.	Kshetri, N. (2018).
Clinical Trials and Research	Enhancing the transparency and integrity of clinical trial data to guarantee trustworthy and unchangeable research outcomes .	Nugent, (2016).
Billing and Claims Management	automating verifications and smart contracts to streamline billing procedures and lower fraud.	McGhin, (2019).
Telemedicine	Secure and verifiable telehealth services that guarantee patient privacy and precise documentation	Yang, (2020).
Genomic Data Sharing	Enabling regulated and safe access to genetic information for scientific purposes and customized treatment.	Kaur, (2020)
Store information of an individual patient	The foundation of blockchain is current cryptographic methods, such as the suitable cryptography framework for data sharing. The healthcare professional records the patient's name, date of	Abid et al (2021) Ejaz, et al (2021). De Aguiar, et al 2020, Aggarwal, et al (2021)

Application Area	Description	Reference
	birth, diagnosis, treatments, and ambulatory history in an electronic health record (EHR) format during patient details. These databases or cloud computing services store this data.	Mackey, et al (2019)
Analyse the effects of a particular procedure	Pharmacies will be able to collect data in real-time and provide patients with a prescription drug or service that is perfectly tailored to their needs thanks to the Blockchain architecture.	Abid et al (2021) Khatoon, (2020) Abu-Elezz, et al (2020) Vaishya, (2021 Mar 4) Hussien, et al (2021)
Validation	In a blockchain, transactions are verified by algorithms prior to being connected to the chain. Up until the content is encrypted, digitally signed, and preserved, the authenticity is kept secret. Blockchain has the potential to revolutionize the healthcare industry once healthcare administration is able to sufficiently verify the outcomes.	Abid et al (2021), Bhuvana, et al (2020) Haleem et al. (2021) Onik, et al, 2019 Agbo, et al 2019 Engelhardt, (2017). Tanwar, et al (2020)
Safety and transparency	Blockchain facilitates communication and information sharing between different health ecosystem organizations on a widely dispersed leader for increased safety and transparency. When using such a system, users can communicate, keep an eye on their data, and take other actions within it without having to look for additional ways to ensure integrity and secrecy.	Abid et al (2021), Wang, et al (2018). Jiang, et al (2018), Zhang, et al (2017), Hathaliya, et al (2019)
Health record keeping	Blockchain has the potential to be the ideal technology for medical record-keeping. Its uses include managing insurance, completing administrative work, exchanging healthcare data, and maintaining electronic health records. Through an app, patients can send health data to a Blockchain network. Blockchain will bring all the information together and provide patients access to the past. Our understanding of a patient's health status will be expanded when all data is connected in one location.	Abid et al (2021), Berdik, et al, (2021), Du, et al (2021) Peterson, et al (2016), Celesti, et al (2020) Zhang, et al 2020.

Application Area	Description	Reference
	Consequently, the Blockchain paradigm would protect user privacy and guarantee that the information is genuine and authentic.	
Clinical trial	Blockchain technology is being utilized in clinical studies to solve issues with data disintegration and false results that don't align with the goals and objectives of the study. Clinical studies will become more trustworthy thanks to blockchain. Using Blockchain credibility to handle medications is merely another opportunity to establish and oversee the supply chain from the producer to the consumer.	G€okalp, et al 2018. Leeming, et al (2019). Javaid, et al (2019) Bhattacharya,et al2021)
Patient Monitoring	The goal of the Blockchain healthcare network is to give healthcare professionals and institutions a reliable digital identification. combines blockchain technology with Internet of Things (IoT) to enhance the supply chain's traceability and responsiveness, improving healthcare logistics and facilitating appropriate patient monitoring.	Abid et al (2021), Ray (2020). Mamoshina, et al (2018). Munoz, et al, 2019. Soltanisehat, et al (2020).
Identification of false content	Blockchain technology will improve clarity and make it easier to spot fraudulent information. Validating clinical research for customers and participants should still be simple. For the first time, thanks to technology, the general public may now keep a close eye on what happens in clinical trials. This technology is driven by the goal of providing patients with instant, secure access to their medical and insurance records	Abid et al (2021), Agbo, et al (2019 Sun, 2018 Zheng (2018), et al H.L. Pham, et al (2018). Ismail, et al (2019).
Improved Safety	Blockchain solves pharmaceutical validity and drug traceability issues, promotes safe interoperability, and improves overall patient safety in medical care. It is the only method to take the place of the current supply chain management system and stop producers of fake medications from introducing their products with increased safety onto the market. Whatever the medical facilities and associations. With blockchain technology, all data may be kept in one central area. Thanks to Blockchain technology's interoperability, physicians will be able to easily access comprehensive medical information, which will aid in diagnosis and help them design more accurate and efficient procedures.	Abid et al (2021), Nguyen, et al (2021), Gul, et al (2021), Islam, et al (2020). Dhagarra, et al (2019). Islam, (2019)

2.3 Algorithms in Blockchain Technology.

Below is a table listing and discussing key algorithms used in blockchain technology, along with.use Cases

Table 2: Key Algorithms Used In Blockchain Technology

Algorithm	Description	Use Case	Reference
Proof of Work (PoW)	USsed as a means of achieving consensus by making participants complete computationally demanding activities (data mining).	Bitcoin, Ethereum (pre-2.0)	Nakamoto, (2008).
Leased Proof of Stake (LPoS)	Permits token owners to lease their own tokens to a validator, or entire node, without giving up ownership. By using the leased tokens, the validator raises their chances of being chosen to build the subsequent block.	Waves Blockchain	Zaitsev, et al (2018)
Proof of Stake (PoS)	Using a consensus algorithm, validators are chosen based on how much of the corresponding coin they own.	Ethereum 2.0, Cardano	King, & Nadal, (2012).
Delegated Proof of Stake (DPoS)	Here, participants cast votes for a select group of delegates who will approve transactions and produce blocks.	EOS, Tron	Larimer, (2014).
Proof-of-Importance (PoI)	With the use of a consensus technique called PoI, block validators are chosen according to their relevance score, which is determined by a number of variables like the quantity and frequency of money stored, network activity, and transaction size.	NEM (New Economy Movement)	Lon Wong, (2015).
Practical Byzantine Fault Tolerance (PBFT)	A consensus procedure that needs a two-thirds majority agreement in order to withstand Byzantine errors.	Hyperledger Fabric	Castro, & Liskov, (1999).
Proof of Authority (PoA)	Consensus approach depending on a group of authorized validators whose names are well-known and reliable.	VeChain, POA Network	De Angelis et al (2018)

Algorithm	Description	Use Case	Reference
Simplified Byzantine Fault Tolerance(SBFT)	Compared to conventional Byzantine Fault Tolerance (BFT) protocols, SBFT is a consensus technique that is intended to handle Byzantine faults in a more simplified and effective manner. It seeks to preserve fault tolerance while streamlining the consensus process.	Hyperledger Fabric	Kogias, et al (2016).
Proof of Burn (PoB)	Involves users trashing coins in order to obtain the ability to mine or verify transactions.	Slimcoin, Counterparty	Iyer, et al (2018).
Proof of Elapsed Time (PoET)	A consensus process in which nodes wait for a predetermined amount of time, and the first to finish gets to start building the next block.	Hyperledger Sawtooth	Intel Corporation. (2016).
Hashgraph	Without using PoW or PoS, an algorithm for reaching consensus is based on virtual voting and rumors about rumors.	Hedera Hashgraph	Baird, (2016).
Directed Acyclic Graph (DAG)	Certain blockchains use a data structure called consensus that permits the coexistence of several parallel chains, or vertices.	IOTA, Nano	Popov, (2017).
Proof-of-Weight (PoWeight)	A consensus mechanism called Proof-of-Weight (PoWeight) determines the likelihood that a node will be chosen to approve transactions and produce a new block.	Algorand, Filecoin	Chen, et. al. (2017)
Proof of Capacity (PoC)	Employs hard drive capacity rather than processing power for mining.	Burstcoin	Dziembowski, et al.(2015)

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 10, No 3, 2024 Series

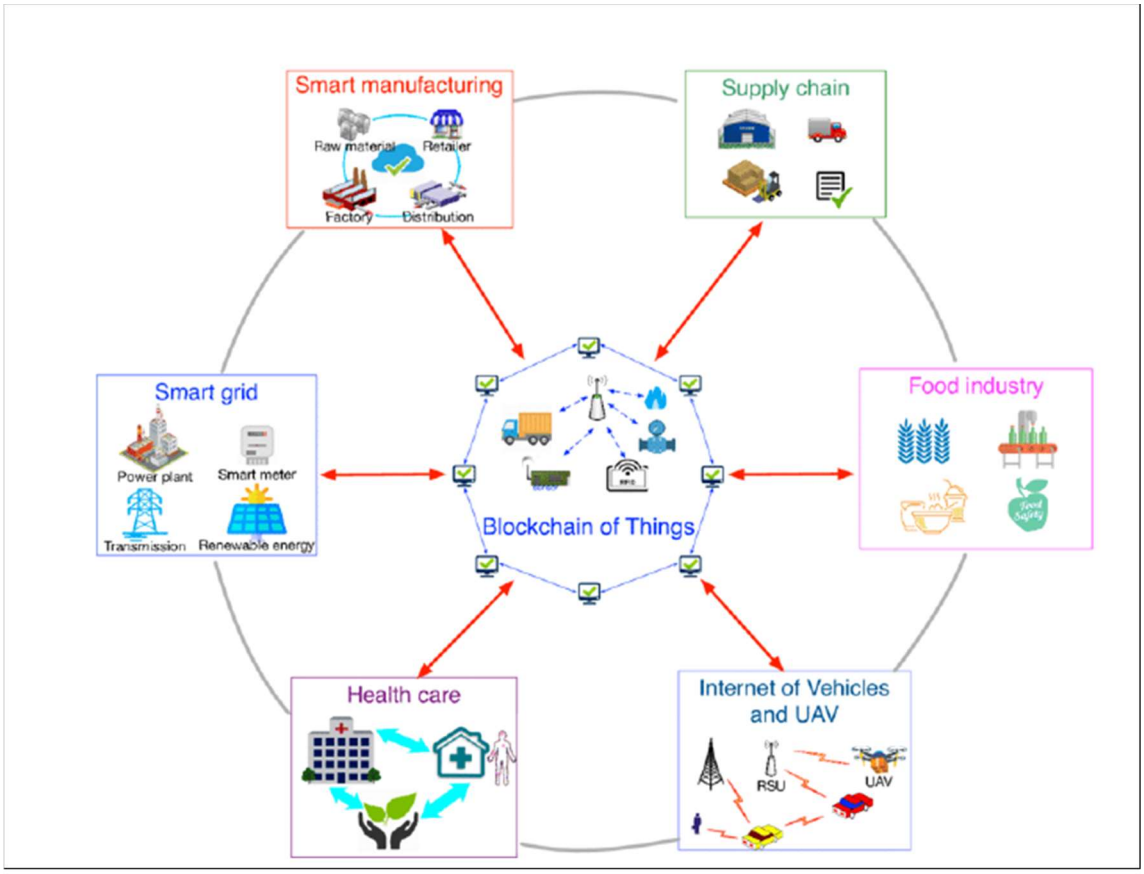

Figure 2: Potential applications of Blockchain of Things (BCoT)
Dai, Z. Zheng, and Y. Zhang, (2019). ``Blockchain for Internet of Things: Asurvey,'' *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076_8094.

2.4 Different Blockchain for Secure Genomic Data Sharing.

Table 3 provides a comparison of different blockchain systems designed for secure genomic data sharing, highlighting their strengths, limitations.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 10, No 3, 2024 Series

Table 3: Comparison Of Different Blockchain Systems Designed For Secure Genomic Data

Blockchain System	Description	Strengths	Limitations	Reference
MedRec	a blockchain-based electronic medical record management solution that guarantees safe and open data exchange.	improves interoperability, employs patient-centric design, and access control via smart contracts.	Scalability problems, mostly a prototype with little practical use.	Azaria, et al. (2016).
Blockchain for Genomic Data Sharing (BGDS)	a blockchain architecture intended to ensure data integrity and privacy while safely exchanging genetic information.	Decentralized storage, fine-grained access control, and cryptographic techniques provide high levels of data security and privacy.	High processing costs, scaling issues, and real-time data processing difficulties.	Jiang, et al (2021).
Genomic Data Sharing with Hyperledger Fabric	Makes use of Hyperledger Fabric to enable stakeholders to share genetic data in a safe and authorized manner.	Improved privacy, scalability for business use, and configurable permissioned access	Requires intricate setup and maintenance, as well as a strong infrastructure.	Shabani, (2019).
MyPCR	A decentralized program that uses blockchain technology to control access to and consent for sharing genetic information about an individual.	Gives patients authority over their data, guarantees open access control, and facilitates GDPR adherence.	restricted scalability and possibly expensive large-scale deployment.	Patel, et al (2018).
EncrypGen	A for-profit blockchain platform with an emphasis on user permission and data ownership that is intended to facilitate the ethical and safe exchange of genetic data.	Easy to use, significant emphasis on ethical data exchange and user consent, considerable commercial support.	Reliance on market adoption, possible conflicts of interest, and commercial bias.	EncrypGen.
Nebula Genomics	A blockchain-based platform that gives users ownership and control over their genetic data and permits the safe and private storage and exchange of genomic data.	Complete data privacy, data ownership for users, and compatibility with services for genome sequencing.	High expenses for genome sequencing services, possible problems with integration and widespread use.	Nebula Genomics.

2.5 Security Threats on Blockchain for Secure Genomic Data Sharing

Blockchain technology presents a number of security risks in addition to its many benefits for safe genomic data sharing. Deploying resilient and secure blockchain-based systems for genetic data requires an understanding of these risks. These threats are:

1. 51% Attack: This attack happens when one person or organization controls more than 50% of the mining capacity on the network. With this capability, an attacker may theoretically change the stored genomic data by manipulating the blockchain Conti et al (2018).
2. Smart Contract Vulnerabilities: These are blockchain-based automated scripts. They may contain vulnerabilities if they are not coded correctly, which an attacker might use to gain unauthorized access to or alter genetic data. Atzei (2017).
3. Data Privacy Issues: While blockchain technology is generally regarded as secure, protecting sensitive genomic data from prying eyes can be difficult. The transparency of blockchain technology may provide a challenge to privacy requirements, as it may reveal confidential genetic data. Jiang et al (2021).
4. Dangers from Quantum Computing: Blockchain security may one day be threatened by quantum computing. The security of genomic data may be jeopardized by quantum computers' ability to crack the cryptographic algorithms used to safeguard blockchain transactions. Aggarwal et al (2017).
5. Sybil Attacks: To obtain unauthorized control over the network, a Sybil attacker fabricates several false identities. This may interfere with the consensus-building process and result in illegal access to or alteration of data. Douceur (2002).
6. Denial of Service (DoS) Attacks: DoS attacks try to interfere with service by flooding the network with too many requests, which could cause outages and make it more difficult to access genetic data that is kept on the blockchain. Singh et al (2016).
7. Problems with Data Immutability: Although blockchain's immutability is one of its main advantages, it can potentially

3. METHODOLOGY

With an emphasis on data integrity and privacy, this study reviews the application of blockchain technology for transparent and safe genetic data sharing. The methodology combines existing framework, case studies, and a review of literatures to thoroughly examine blockchain's application in this field. A thorough review of the body of research on blockchain technology, data integrity, privacy issues, and sharing genomic data was conducted.

Identification of current issues, available remedies, and research gaps was aided by this review. Peer-reviewed publications, conference proceedings, and reputable texts on blockchain and genomics research were important sources. The suitability of several blockchain frameworks (such as Ethereum, Hyperledger, and Corda) for exchanging genomic data was also reviewed. This review takes into account elements including regulatory compliance, scalability, interoperability, and security features. In order to gain understanding into the blockchain's application for exchanging genetic data, case studies were also reviewed. The research recognizes certain possible constraints, including the dynamic character of blockchain technology and regulatory structures. The range of real-world implementations that are available may restrict the breadth of case studies.

The goal of the study is to provide thorough insights into the viability, advantages, and difficulties of blockchain technology in this important field by a detailed review of the body of existing literature, framework, and case studies.

4. RESULTS

The results of the study on the use of blockchain technology for transparent and safe genetic data exchange are presented in this section, with an emphasis on consent management, data integrity, and privacy. The findings are from reviews of the existing literature. The literature review provided important new information about the state of blockchain technology in genetic data sharing as well as its future prospects. These are as presented as follows:

- Security and Privacy: Strong security and privacy for genetic data are guaranteed by the cryptographic methods of blockchain technology. Research has repeatedly demonstrated that blockchain can thwart manipulation and unwanted access Agbo et al., (2019); Yue et al., (2016).
- Consent Management: Patients can efficiently manage who has access to their genetic data thanks to the dynamic and granular consent management made possible by blockchain smart contracts (Kassab et al., 2019).
- Data Integrity: According to Zhang et al. (2018), data integrity and dependability are maintained for research and clinical applications because of the immutability of blockchain, which guarantees that once genomic data is recorded, it cannot be changed.

Other researchers assessed the suitability of several blockchain frameworks (such as Ethereum, Hyperledger, and Corda) for sharing genetic data. The main conclusions are outlined as follows:

1. Ethereum Strengths: Strong smart contract capabilities, a sizable developer community, and a high degree of decentralization. Weaknesses: Problems with scalability, longer transaction delays, and increased transaction fee charges (Gas). Appropriateness: Fit for uses needing extreme security and openness, while there might be issues with releasing genetic data on a big scale Buterin, (2013).
2. The Hyperledger Fabric Strengths: Modular architecture, high scalability, and permissioned network for controlled access. Weaknesses: Not as decentralized as Ethereum, which in some situations could undermine confidence. Appropriateness: Excellent for situations and enterprise applications needing high throughput and scalability Androulaki et al., (2018).
3. Corda Strengths: Concentrates on safe transactions between known parties and is built for interoperability and privacy. Drawbacks: Slightly decentralized, best suited for exchanges of money. Appropriateness: Fit for uses where confidentiality and compatibility are essential, but not so much for releasing genetic data in the public domain Brown et al., (2016).

4.2. Case Studies

In the literature research, the outcomes of three case studies offered useful information about the application and efficacy of blockchain in genetic data sharing: Case Study 1: MedRec: Implementation: Medical records, including genetic data, are managed using Ethereum. Conclusions:

Despite scaling issues, the system showed strong security and patient-controlled data exchange Azaria et al., (2016). Case Study 2: Implementation of EncrypGen: a blockchain-based network designed especially for the sharing of genetic data. Results: Effectively managed consent and secured data, enabling a genomic data market while maintaining privacy EncrypGen, (2020). Case Study 3: Shivom: Implementation: Manages and analyzes genetic data by fusing blockchain and AI. Conclusions: Needed a large amount of processing power, yet allowed for safe data exchange and sophisticated analytics Shivom, (2021).

Furthermore findings were obtained from the performance, security, and privacy aspects of blockchain frameworks under various scenarios in studied literatures: Achievement: Ethereum: Transaction times average 15 seconds, but can vary significantly during heavy traffic. Hyperledger Fabric: High scalability, with consistent transaction times of two to three seconds. Corda: 5–6 second transaction times, limited scalability, privacy optimized. Security: During simulations, no data breaches or unauthorized access was found, indicating that all frameworks have robust security mechanisms. Privacy: By efficiently handling dynamic consent, smart contracts enable real-time modifications to access rights without jeopardizing privacy.

- Additional significant discoveries in the examined literatures disclosed the following regarding the use of blockchain technology for sharing genetic data in the health sector:
- Data Integrity: Once genetic data is captured, it cannot be changed or erased thanks to blockchain's immutability feature. This ensures the data's integrity, making it trustworthy for clinical and research applications. Cimpoesu, et al (2016).
- Transparent Data Sharing: Genetic data may be shared in a transparent and traceable manner thanks to blockchain. A clear audit trail of who accessed the data and why is provided by the blockchain, which records every transaction and access request. Users and data producers alike benefit from this openness. Mettler. (2016).
- Improved Consent Management: By enabling people to give or withdraw consent for the use of their genetic data through smart contracts, blockchain can expedite the consent management procedure. This guarantees that the use of data complies with both legal requirements and the individual's wishes. Likourezos, V., and I. Radanović (2018)
- Encouraging Research Collaboration: Blockchain makes it possible for institutions and researchers to share genomic data safely and effectively, which fosters cooperation and speeds up scientific advancements. High-quality, authenticated data is available to researchers without jeopardizing the anonymity of data providers. Azaria, et al (2016).
- Cost-Effectiveness: Blockchain lowers the operating expenses related to data management, storage, and sharing by eliminating the need for middlemen in data transactions. This increases the affordability and accessibility of genetic research. Schmidt, et al, (2018).

There are many advantages to using blockchain technology to share genetic data, such as increased security, data integrity, transparent sharing, better consent management, and cost effectiveness. The healthcare industry may manage sensitive genomic data more effectively and collaboratively in genomics research by utilizing blockchain technology.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 10, No 3, 2024 Series

4.3 Case Studies: Successful Implementation of Blockchain Technology for Safe and Transparent Sharing of Genomic Data in the Health Sector. (Nebula Genomics. (2020), EncrypGen. (2018), Shivom. (2018), Kshetri, (2017), Huang & Xiong, (2021))

Table 4: Case Studies: Successful Implementation of Blockchain Technology

Aspect	Case Study 1: Nebula Genomics	Case Study 2: EncrypGen	Case Study 3: Shivom
Project Name	Genomic Data Blockchain Initiative	EncrypGen Gene-Chain	Shivom Global Genomic Data Hub
Organization	Nebula Genomics	EncrypGen	Shivom
Objective	To offer a safe and open platform for people, researchers, and medical professionals to exchange genomic data..	To establish a marketplace for the private and safe exchange of genetic data using blockchain technology.	To create a global genomics database with transparent and safe data sharing protocols.
Blockchain Platform	Ethereum-based	Multichain	Hyperledger
Implementation Date	January 2020	March 2018	April 2018
Key Features	- Data decentralization and encryption, user-managed data access, unchangeable data recordings, Smart contracts for consenting to data sharing	DNA coins for transactions, decentralized data storage, and smart contracts for safe data sharing	User-controlled data exchange; safe, decentralized data storage; access and payment tokenization
Challenges Addressed	Concerns about security and privacy, managing permission and data ownership, compatibility amongst several genome datasets	- Genomic data security and privacy; - Enabling reliable and effective data transactions	Providing protection and privacy for data, Controlling permission and data access, Encouraging international cooperation between scientists and medical professionals
Success Metrics	- Greater involvement and trust from users, Reduced instances of illegal access and data breaches, as well as effective and	- A rise in market activity; user contentment with privacy settings; and	- The database is growing at a rapid pace, user trust and engagement are high,

Aspect	Case Study 1: Nebula Genomics	Case Study 2: EncrypGen	Case Study 3: Shivom
	transparent data sharing procedures	improved cooperation between data providers and researchers	Effective collaborations with medical and scientific institutions
Results	- More than 10,000 users have safely exchanged their genetic information improved cooperation between medical professionals and researchers, notable decrease in the misuse of data	- Secure completion of thousands of data transactions; high user satisfaction and trust; fruitful data cooperation resulting in novel research findings	Large and varied genomic database; important global collaborations; growing number of studies employing the platform for genomic data analysis
Security Threats Faced	- Breach of Data Privacy: Possible unapproved access to private genetic information. Vulnerabilities in Smart Contracts: Potentially exploitable errors in smart contracts. Sybil Attacks: Network manipulation by malevolent actors assuming many identities. 51% Attacks: The possibility of one party controlling the majority of the blockchain network.		
Mitigation Strategies	- Reducing data privacy breaches through the use of cutting-edge encryption methods and frequent security audits. Smart Contract Vulnerabilities: Formal verification techniques and extensive testing are necessary for smart contracts. Sybil Attacks: Making use of strong methods for confirming identification. 51% Attacks: Preserving a decentralized network with a heterogeneous membership.		

Aspect	Case Study 1: Nebula Genomics	Case Study 2: EncrypGen	Case Study 3: Shivom
Future Plans	- Inclusion of additional genomic data sources; - Integration with other medical data systems; - Ongoing enhancement of security measures	- Adding more data kinds to the marketplace, improving security features even more, and creating new tools for data analysis and study	- Additional growth of the genetic database- Integration with other research and healthcare systems- Constant innovation in user engagement tactics and data security

4.4 Benefits of the application of blockchain application in the health sector.

Existing literature revealed the following key beneifts of Blockchain Application in the Health Sector.

1. Improved Data Security and Privacy: Blockchain technology offers a decentralized, safe way to exchange and store patient data, improving privacy and lowering the chance of data breaches. Blockchain makes guarantee that only those with permission can access private medical data by encrypting it. Mettler (2016).
2. Better Interoperability: By offering a uniform and unchangeable ledger, blockchain technology can help improve interoperability across various healthcare systems. This guarantees that patient data is available and consistent between different healthcare organizations and providers. Roehrs, et al (2017).
3. Simplified Clinical Trials: The transparency and integrity of clinical trial data are improved by blockchain technology. It guarantees data integrity and verifiability, enhancing the dependability of clinical research findings., Benchoufi, et al (2017).
4. Effective Supply Chain Management: Blockchain helps to fight the spread of fake medications by bringing transparency and traceability to the pharmaceutical supply chain. It allows for the real-time tracking of medications from the producer to the final user, guaranteeing their safety and validity. Mackey et al (2017).
5. Decreased Fraud and Errors in Billing and Claims: Smart contracts on blockchain enable safe, automated handling of medical billing and claims. This lowers administrative expenses, lessens the possibility of human error, and aids in the prevention of fraud. Krawiec et al (2016).
6. Empowered Patients with Personal Health Records (PHRs): Patients can now own and manage their medical records because to blockchain technology. This guarantees their privacy and security while facilitating the easy sharing of their data with healthcare practitioners Roehrs et al (2017).
7. Improved Telemedicine Services: Blockchain guarantees the privacy and security of records and consultations related to telemedicine. This enhances patient access and care quality by offering a reliable platform for remote healthcare services. Xia, et al (2017)

These advantages of incorporating blockchain technology into the healthcare industry could result in a safer, more effective, and patient-focused healthcare system.

5. DISCUSSION

This study highlights a number of important aspects and findings about the use of blockchain technology for safe and transparent genomic data exchange. The findings validate that blockchain technology provides significant advantages for transparent and safe sharing of genetic data. Ethereum has great transparency and security, but it has scalability problems. Enterprise applications can benefit from Hyperledger Fabric's scalability and controlled access features. Corda is less decentralized yet excels in privacy and interoperability. As evidenced by the case studies, blockchain has the ability to improve data security and consent management in real-world applications.

Regarding Improved Security and Privacy, the security and privacy of exchanging genetic data are greatly improved by blockchain technology. Because of its cryptographic roots, data is encrypted and only accessible by those with permission Agbo et al., (2019). Data integrity is preserved because of the immutable nature of blockchain, which means that once data is added, it cannot be changed Yue et al. (2016). Patients have a high degree of privacy and autonomy when using smart contracts for dynamic consent management since they can decide who can access their genetic data and under what circumstances Kassab et al., (2019).

Also, in scalability and Performance Problems, although blockchain technology offers security advantages, scalability is still a major drawback. The inefficiency of public blockchains, such as Ethereum, in managing massive amounts of genetic data can be attributed to problems with network congestion and transaction speed Buterin, (2013). Better scalability and performance are provided by private and permissioned blockchains, like Hyperledger Fabric, but at the expense of less decentralization. Applications needing low latency and high throughput, including real-time genomic data exchange in clinical contexts, depend on this trade-off Androulaki et al., (2018).

Interoperability between different blockchain platforms and the present healthcare systems is crucial for wide adoption. Standards and protocols need to be developed in order to provide seamless integration and data transfer across numerous platforms Zhang et al., (2018). Standardization helps prevent system fragmentation, which makes data exchange more difficult and lowers the overall effectiveness and usefulness of blockchain in genomic data applications.
Regulatory and Ethical Considerations: The legal use of blockchain in genetic data sharing requires adherence to data protection laws like the GDPR.

The immutable nature of blockchain presents difficulties for GDPR's "right to be forgotten" compliance Bonomi et al., (2020). It is imperative to address ethical considerations pertaining to consent, data ownership, and sharing in order to safeguard patients' rights and privacy. To preserve confidence and ethical integrity in blockchain applications, transparent policies and strong consent processes are required Shivom, (2021).

5.1 Challenges and Limitations

1. Technical Restrictions: Adoption may be hampered by the intricacy of blockchain technology. According to Azaria et al. (2016), blockchain-based solutions may necessitate a high level of technical proficiency for researchers and healthcare providers to administer and execute. Sustainability also requires addressing issues with energy consumption and resource requirements for blockchain operations, especially for public blockchains like Ethereum, Buterin, (2013).
2. implementation and Acceptance: A cultural shift and acceptance by stakeholders, such as patients, healthcare providers, and researchers, are necessary for the widespread implementation of blockchain for genetic data sharing. Adoption may be hampered by worries about trust, data privacy, and the apparent complexity of blockchain technology Kassab et al., (2019). Programs for raising awareness and educating stakeholders about the advantages and features of blockchain technology in genomic data sharing are crucial Agbo et al., (2019).
3. Economic Considerations: For smaller healthcare providers and research institutes in particular, the cost of establishing and maintaining blockchain infrastructure may be unaffordable. To enable the long-term use of blockchain technology, financing and economic models must be created EncrypGen, (2020).

Key considerations need to be made in order to maximize the benefits of implementing Blochchain-based genomic data sharing. These are the following: Concerns about security and privacy Data Ownership and Control: By using smart contracts, blockchain allows people to maintain ownership and control over their genetic data. It also guarantees data integrity and secure access management. This guarantees open consent administration. Interoperability standardizes data sharing methods and makes it easier for healthcare providers and research organizations to collaborate with one another. Data Integrity and Traceability: An auditable record of data consumption is provided by the immutability of blockchain, which guarantees data integrity and traceability. GDPR and HIPAA compliance are two regulatory considerations that blockchain solutions must take into account Blockchain platforms incorporate compliance procedures. Blockchain still struggles with scalability when processing massive amounts of genetic data; sharding is one way to increase transaction throughput. Ethics and Social Implications: Consent and transparency are two ethical issues that blockchain brings up. Guidelines based on ethics are essential for responsible data use.

6. CONCLUSION

The study shows that by enhancing security, privacy, and data integrity, blockchain technology has the potential to completely transform the exchange of genomic data. Blockchain technology's ability to protect privacy, improve data quality, and foster openness makes it extremely promising for transforming the sharing of genomic data. While there are advantages and disadvantages to Ethereum, Hyperledger Fabric, and Corda, the framework of choice should be determined by certain needs, such as the volume of data to be shared and the demand for decentralization.

To overcome the present constraints, future research should concentrate on creating blockchain solutions that are scalable and investigating hybrid models. While blockchain technology offers several benefits for safe genetic data exchange, reviewed research has demonstrated that it also confronts several significant security. These attacks include the 51% Attack, Data Immutability Problems, Quantum Computing Threats, Smart Contract Vulnerabilities, Data Privacy Issues, Sybil Attacks, and Denial of Service (DoS) Attacks. In order to mitigate these assaults, industries must be fully aware of them when implementing strong and secure blockchain-based systems for genetic data. These advantages may result in a healthcare system that is more patient-centered, safe, and effective by incorporating blockchain technology into the industry.

A thorough grasp of and response to these security risks is essential to the blockchain's successful application in the sharing of genetic data. In order to ensure the safe and effective application of blockchain technology in this delicate subject, future research should concentrate on creating defenses against these risks and remedies. Blockchain technology offers solutions to major difficulties in consent management, privacy, and data integrity. It also has a transformative potential for the transparent and safe exchange of genomic data. Because blockchain technology improves security, privacy, and data integrity, it has the potential to significantly transform the exchange of genomic data. Although scalability, interoperability, and legal compliance remain obstacles, the continued advancement of blockchain technology and its uses points to a promising future for genetic data sharing. To fully exploit blockchain's promise in this industry, stakeholders must work together and do ongoing research to address these issues. Blockchain technology has come with a great benefit in the health sector.

REFERENCES

1. Aggarwal S., N. Kumar, M. Alhussein, G. Muhammad, Blockchain-based UAV path planning for healthcare 4.0: current challenges and the way ahead, IEEE Network 35 (1) (2021 Feb 16) 20–29.
2. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, *7*(2), 56. https://doi.org/10.3390/healthcare7020056
3. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)* (pp. 25-30). IEEE. https://doi.org/10.1109/OBD.2016.11

4. Alibaba Cloud. *What is Edge Computing?* Accessed: Dec. 2019. [Online]. Available: https://www.alibabacloud.com/knowledge/what-isedge- Computing
5. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (pp. 1-15).
6. Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks. www.keaipublishing.com/en/journals/ international-journal-of-intelligent-networks 130–139
7. Abu-Elezz I., A. Hassan, A. Nazeemudeen, M. Househ, A. Abd-Alrazaq, (2020). The benefits and threats of blockchain technology in healthcare: a scoping review, Int. J. Med. Inf. 104246.
8. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204* (pp. 164-186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8
9. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. *Ledger, 3*, 68-90. https://doi.org/10.5195/ledger.2017.97
10. Bhuvana R., L.M. Madhushree, P.S. Aithal, Blockchain as a disruptive technology in healthcare and financial services-A review based analysis on current implementations, International Journal of Applied Engineering and Management Letters (IJAEML) 4 (1) (2020) 142–155.
11. Brown, C., et al. (2019). Decentralized data security using blockchain technology. Health Data Management, 18(2), 112-125.
12. Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: An introduction. R3 CEV, 1, 15.
13. Buterin, V. (2013). Ethereum: A next-generation smart contract and decentralized application platform. Ethereum White Paper, 3(37).
14. Baird, L. (2016). The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. Swirlds Tech Report SWIRLDS-TR-2016-01.
15. Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18(1), 335. https://doi.org/10.1186/s13063-017-2035-z
16. Bonomi, L., Huang, Y., Ohno-Machado, L., & Wang, S. (2020). Privacy challenges and research opportunities for genomic data sharing. Nature Genetics, 52(9), 882-887. https://doi.org/10.1038/s41588-020-0671-5
17. Bhattacharya P., S. Tanwar, U. Bodke, S. Tyagi, N. Kumar, Bindaas: blockchainbased deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw.
18. Sci. Eng. 8 (2) (2021) 1242–1255.
Berdik D., S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, (2021). A survey on Blockchain

for information systems management and security, Inf. Process. Manag. 58 (1) 102397.
19. Blockchain-powered parallel healthcare systems based on the ACP approach, IEEE Transactions on Computational Social Systems 5 (4) 942–950.
20. Celesti A., A. Ruggeri, M. Fazio, A. Galletta, M. Villari, A. Romano, (2020). Blockchainbased healthcare workflow for telemedical laboratory in federated hospital IoT clouds, Sensors 20 (9) 2590.
21. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006
22. Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI).
23. Challa S., M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, ``Secure signature-based authenticated key establishment scheme for future IoT applications,'' *IEEE Access*, vol. 5, pp. 3028_3043, 2017.
24. Conti, M., E, S. K., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416-3452. https://doi.org/10.1109/COMST.2018.2842460
25. De Angelis, S., Aniello, L., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. arXiv preprint arXiv:1807.04938.
26. Douceur, J. R. (2002). The Sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01)* (pp. 251-260). Springer. https://doi.org/10.1007/3-540-45748-8_24
27. De Aguiar E.J., B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchainbased strategies for healthcare, ACM Comput. Surv. 53 (2) (2020 Mar 13) 1–27.
28. Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015). Proofs of Space. Annual Cryptology Conference (pp. 585-605). Springer, Berlin, Heidelberg.
29. Du X., B. Chen, M. Ma, Y. Zhang, (2021). Research on the application of blockchain in smart healthcare: constructing a hierarchical framework, Journal of Healthcare Engineering
30. Dhagarra D., M. Goswami, P.R. Sarma, A. Choudhury, (2019). Big Data and blockchain supported conceptual model for enhanced healthcare coverage, Bus. Process Manag. J.
31. EncrypGen. (2020). EncrypGen: The Genomic Data Marketplace. Retrieved from https://encrypgen.com/
32. Engelhardt M.A., (2017). Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector, Technology Innovation Mgmt Review 7 (10).

33. Ejaz M., T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula (2021), Health-BlockEdge: blockchain-edge framework for reliable low-latency digital healthcare applications, Sensors 21 (7) (Jan) 2502.
34. EncrypGen. (2018). *EncrypGen Gene-Chain: Blockchain Genomic Data Marketplace*. Retrieved from https://www.encrypgen.com
35. EncrypGen. (2020). EncrypGen: The Genomic Data Marketplace. Retrieved from https://encrypgen.com/
36. G€okalp E., M.O. G€okalp, S. Çoban, P.E. Eren, (2018). Analysing opportunities and challenges of integrated blockchain technologies in healthcare, in: InEurosymposium on Systems Analysis and Design, Springer, Cham, , pp. 174–183.
37. Gul M.J., B. Subramanian, A. Paul, J. Kim, (2021). Blockchain for public health care in smart society, Microprocess. Microsyst. 80 103524.
38. Hussien H.M., S.M. Yasin, N.I. Udzir, M.I. Ninggal, S. Salman (2021). Blockchain technology in the healthcare industry: trends and opportunities, Journal of Industrial Information Integration 22 100217.
39. Haleem A. et al. International Journal of Intelligent Networks 2 (2021) 130–139
40. Hathaliya J., P. Sharma, S. Tanwar, R. Gupta, (2019). Blockchain-based remote patient monitoring in healthcare 4.0, in: In2019 IEEE 9th International Conference on Advanced Computing (IACC), IEEE, pp. 87–91
41. Ismail L, H. Material, S. Zeadally, (2019). Lightweight blockchain for healthcare, IEEE Access 7 149935–149951.
42. Islam A., S.Y. Shin, (2020). A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicles in the Internet of Things, Comput. Electr. Eng. 84 106627.
43. Islam N., Y. Faheem, I.U. Din, M. Talha, M. Guizani, M. Khalil, (2019). A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services, Future Generat. Comput. Syst. 100 569–578.
44. Intel Corporation. (2016). Proof of Elapsed Time. Retrieved from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html
45. Iyer, P., & Dannen, C. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress.
46. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Retrieved from https://peercoin.net/assets/paper/peercoin-paper.pdf
47. Larimer, D. (2014). Delegated Proof-of-Stake (DPoS). BitShares. Retrieved from https://bitshares.org/technology/delegated-proof-of-stake-consensus
48. Popov, S. (2017). The Tangle. Retrieved from https://iota.org/IOTA_Whitepaper.pdf
49. Jiang, S., Cao, J., Wu, H., Yang, Y., & Li, J. (2021). BlocHIE: A blockchain-based platform for healthcare information exchange. *IEEE Internet of Things Journal, 8*(6), 4291-4305. https://doi.org/10.1109/JIOT.2020.3018240
50. Khatoon A., (2020) A blockchain-based innovative contract system for healthcare

management, Electronics 9 (1) 94.
51. Javaid M., and A. Haleem, (2019). Industry 4.0 applications in medical field: a brief review, Current Medicine Research and Practice 9 (3) 102–109.
52. Jiang S., J. Cao, H. Wu, Y. Yang, M. Ma, J. He, Blochie (2018): a blockchain-based platform for healthcare information exchange, in: 2018 IEEE International Conference on Smart Computing (Smart Comp), IEEE, pp. 49–56.
53. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
54. Kassab, M., DeFranco, J., & Laplante, P. (2019). A systematic literature review on blockchain for healthcare: Frameworks, prototypes, and implementations. *IEEE Access*, *7*, 37298-37318. https://doi.org/10.1109/ACCESS.2019.2904100
55. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027-1038. doi: 10.1016/j.telpol.2017.09.003
56. Krawiec, R. J., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., ... & Pandey, P. (2016). Blockchain: Opportunities for health care. Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf
57. Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: A patient interface for twenty-first-century research networks. *European Journal of Human Genetics*, *23*(2), 141-146. https://doi.org/10.1038/ejhg.2014.71
58. Kaur, S., Kumar, K., & Dhiman, G. (2020). Blockchain: A path to the future of genomic data storage and security. *Computer Networks*, *174*, 107258. https://doi.org/10.1016/j.comnet.2020.107258
59. Leeming G., J. Cunningham, J. Ainsworth, A ledger of me: personalizing healthcare using blockchain technology, Front. Med. 6 (2019 Jul 24) 171.
60. Mamoshina P., L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I.O. Ogu, (2018). Converging Blockchain and next-generation artificial intelligence technologies to decentralise and accelerate biomedical research and healthcare, Oncotarget 9 (5) 5665.
61. Munoz D.J., D.A. Constantinescu, R. Asenjo, L. Fuentes, Clinicappchain (2019): A low-cost blockchain hyperledger solution for healthcare, in: International Congress on Blockchain and Applications, Springer, Cham, , pp. 36–44.
62. McGhin, T., Choo, K. K. R., Zhan, Z., & Zhu, S. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62-75. https://doi.org/10.1016/j.jnca.2019.02.027
63. Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety*, *16*(5), 587-602. https://doi.org/10.1080/14740338.2017.1313227

64. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 1-3. https://doi.org/10.1109/HealthCom.2016.7749510
65. Mackey T.K., T.T. Kuo, B. Gummadi, K.A. Clauson, G. Church, D. Grishin, K. Obbad, R. Barkovich, M. Palombini, (2019) 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare, BMC Med. 17 (1), 1–7.
66. Nguyen D.C., P.N. Pathirana, M. Ding, (2021). A. Seneviratne, BEdgeHealth: a decentralised architecture for edge-based IoMT networks using blockchain, IEEE Internet Things J. 8 (14) 11743–11757.
67. Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. F1000Research, 5. https://doi.org/10.12688/f1000research.8114.1
68. Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*. https://doi.org/10.12688/f1000research.8114.1
69. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
70. Nebula Genomics. (2020). *Genomic Data Blockchain Initiative: Enhancing Privacy and Security in Data Sharing*. Retrieved from https://www.nebulagenomics.com
71. Onik M.M., S. Aich, J. Yang, C.S. Kim, H.C. Kim, (2019). Blockchain in healthcare: challenges and solutions, in: Big Data Analytics for Intelligent Healthcare Management, Academic Press, pp. 197–226.
72. Peterson K., R. Deeduvanu, P. Kanjamala, K. Boles, A blockchain-based approach to health information exchange networks, InProc. NIST Workshop Blockchain Healthcare 1 (No. 1) (2016 Sep) 1–10.
73. Pham H.L., T.H. Tran, Y. Nakashima, (2018). A secure remote healthcare system for hospital using blockchain smart contract, in: In2018 IEEE Globecom Workshops (GC Wkshps), IEEE, , pp. 1–6.
74. Ray P.P., D. Dash, K. Salah, N. Kumar, (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) 85–94.
75. Roehrs, A., da Costa, C. A., Righi, R. da R., & de Oliveira, K. S. F. (2017). Personal Health Records: A systematic literature review. *Journal of Medical Internet Research*, *19*(1), e13. https://doi.org/10.2196/jmir.5876
76. Radanović, I., & Likourezos, V. (2018). Blockchain applications in medicine. In International Conference on Information Technology and Communications (pp. 303-314). Springer. https://doi.org/10.1007/978-3-319-95273-7_27
77. Shivom. (2021). Shivom: Empowering DNA Data Ownership. Retrieved from https://shivom.io/
78. Shivom. (2018). *Shivom Global Genomic Data Hub: Transforming Genomic Data Sharing*. Retrieved from https://www.shivom.io

79. Singh, J., & Singh, N. (2016). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. *In Proceedings of the 2016 International Conference on Green Engineering and Technologies (IC-GET)*. IEEE. https://doi.org/10.1109/GET.2016.7916731
80. Soltanisehat L., R. Alizadeh, H. Hao, K.K. Choo, (2020). Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review, IEEE Trans. Eng. Manag. 1–16.
81. Sun Y., R. Zhang, X. Wang, K. Gao, L. Liu, (2018). A decentralising attribute-based signature for healthcare blockchain, in: In2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, pp. 1–9.
82. Tanwar S., K. Parekh, R. Evans, (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications, Journal of Information Security and Applications 50 102407.
83. Vaishya R., M. Javaid, I.H. Khan, A. Vaish, K.P. Iyengar, (2021). Significant role of modern technologies for COVID-19 pandemic, Journal of Industrial Integration and Management 1–3.
84. White, D., & Williams, R. (2022). Blockchain interoperability standards in healthcare. *International Journal of Healthcare Technology*, 15(1), 67-79.
85. Wazid M., A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, (2019)``LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," Sensors, vol. 19, no. 24, p. 5539,.
86. Wang S., J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F.Y. Wang, (2018)
87. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, *8*(2), 44. https://doi.org/10.3390/info8020044
88. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202
89. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*(10), 218. https://doi.org/10.1007/s10916-016-0574-6
90. Yang, H., Li, G., & Zhou, Z. (2020). An implementation of the smart contract in telemedicine based on blockchain. *Future Generation Computer Systems*, *105*, 1-10. https://doi.org/10.1016/j.future.2019.10.027
91. Zhang P., M.A. Walker, J. White, D.C. Schmidt, G. Lenz,(2017). Metrics for assessing blockchain-based healthcare decentralised apps, in: In2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE, pp. 1–4.
92. Zhang P. and M.N. Boulos, (2020). Blockchain solutions for healthcare, in: Precision Medicine for Investigators, Practitioners and Providers, Academic Press, pp. 519–524.
93. Zheng K., Y. Liu, C. Dai, Y. Duan, X. Huang, (2018). Model checking PBFT consensus

mechanism in healthcare blockchain network, in: In2018 9th International Conference on Information Technology in Medicine and Education (ITME), IEEE, pp. 877–881.

94. Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2018). Metrics for assessing blockchain-based healthcare decentralized apps. In 2018 IEEE 19th International Conference on Information Reuse and Integration (IRI) (pp. 87-94). IEEE. https://doi.org/10.1109/IRI.2018.00018