International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2019): 0.28 | SJIF (2019): 7.583

Blockchain Technology: A Paradigm Shift in Data Integrity and Security

Siva Karthik Devineni

Database Consultant, MD, USA

Abstract: ***The Digital Age has been accompanied by a key issue of data protection saved in the cloud. In this paper, which is titled as "Blockchain technology: A paradigm shift in data integrity and security" we look at how blockchain, an emerging but quickly evolving technology, provides high solutions to such a challenge. Blockchain was first created as a shared public ledger for documenting Bitcoin transactions but lately has also gone beyond cryptocurrencies. It has potential applications in digital assets, smart contracts, record keeping, ID systems, and most notably, cloud storage. The main emphasis of this study is the function of blockchain in securely storing, retrieving, and sharing files in decentralized networks. In this paper, the authors seek to study the adoption of blockchain technology within cloud storage and how data security and management can be improved through decentralization, immutability, and cryptographic security which are characteristic of blockchain.***

Keywords: Blockchain, Data Integrity, Security, Cloud Storage, Paradigm Shift, Digital Age, Cryptocurrencies, Smart Contracts, Record Keeping, ID Systems, Decentralization, Immutability, Cryptographic Security, Clark & Wilson Model, Proprietary Private Chain, Infrastructure as a Service (IaaS), Zeppar, Frontend, Backend, Transaction Processing, ABRAXAS, Client - Server Model, Distributed Architecture, Third - Party Auditors (TPA), Provable Data Possession (PDP), Consensus Algorithms, Cryptographic Hash Functions, Decentralized Network, Data Tampering, Data Verification, Challenges, Integration, Scalability, Real - Time Monitoring, User Isolation, Momentary Asset Transfer, Modular Core.

1. Introduction

BLOCKCHAIN Technology is a decentralized database or a transparent open book of all transactions and digital events so - called, being performed and consecutively kept by individuals actively joined together [1]. The consensus is achieved by the process of each transaction within this ledger being authenticated by a majority of the participants of the system. This is to make sure that data that gets into the blockchain is permanently fixed into it and made unchangeable, giving way to a trustful and auditable history of any transaction undertaken [2, 3].

The use of blockchain is much wider than cryptocurrencies. More and more people are seeing opportunities for development with the help of this technology in many other fields, which include smart contacts, data storage, identity verification systems, record keeping and the cloud, etc [4].
In this research project, our interests shift to the use of blockchain technology in guaranteeing data integrity. To resolve this, we point to the model formulated by Clark & Wilson outlining the necessary characteristics of a system which can be considered secure when it comes to the integrity of data. This model includes several critical factors: propertransactions, separation of duties, authentication, company, objective, least benefit, objective control, privilege transfer administration [5, 6, 7].

Our primary interest lies in the development of a proprietary private chain Infrastructure as a Service (IaaS) platform, which we have named "Zeppar. " This platform is conceived to parallel existing services like Storage and Bigchain (DB), with a key differentiation: greater emphasis on the integrity of the data. Our model therefore seeks to review and emphasize the relative importance of the factors listed by Clark and Wilson, in achieving and sustaining integrity of data. It is notable that this section carries a more comprehensive analysis of a properly strong transactions, separation of duties, solid authentication protocols, thorough auditing processes, minimum principle practice, and subject control, and work rights management. We intend to show how such components facilitate the improvement of the entire process, especially in the case of the cloud storage environment, and how all of them are incorporated within the blockchain framework as the case with the data integrity principles lo ensure its highest value [8, 9].

2. Literature Review

There is a widespread assumption among users of cloud computing that encryption data before transferring it to cloud storage ensures a sufficient level of protection. Encryption helps to protect data confidentiality from internal risks, but does not ensure protection from corruption risks due to system misconfigurations or software bugs. In this section, we focus on the traditional methods for data integrity validation for cloud systems; however, they have their limitations, which requires more powerful solutions [10].

Client - side checks or third party audits are the traditional approaches to remote data security. It is the use of MAC algorithms and one of the most common client - side methods is it. For this purpose, these algorithms apply a secret key and data of varying length, which is applied on the client side to detect any accidental or malicious data modification. After generating a MAC, the data owner uploads the data to the cloud. To check integrity the owner re - downloads the data, recalculates the MAC, and compares it with the original MAC. This method is however extremely burdensome, particularly for large files because it requires consuming quite a lot of bandwidth and time for re - downloading data and MAC computation [11].
The second technique utilizes hash trees for data integrity verification. This approach builds a tree from bottom to top where leaf nodes are data and parent nodes are the hashes of

the child nodes until a single root hash is formed. Data owners retain the only root hash. In order to ensure data integrity, they need only to compare the root hash received from the cloud service with the one they possess. But this approach also has practical constraints, in particular, when working with enormous sets, since it requires significant computing resources. Second, if the cloud service only provides storage without computation abilities, users have to switch to download via the client site or heavily depend on other third parties, resulting in wasting a huge amount of bandwidth [12]. As these difficulties, remote data auditing techniques have attracted more attention. Such approaches help to validate the integrity and validity of remote data storage more economically. The advantage of remote data auditing stems from its ability to replace integrity verification, which would otherwise be necessary, and reduce computational costs as well as bandwidth while ensuring that the storage remains secure in a cloud [13].

a) Role of Third - Party Auditors (TPA) in Data Integrity

Third - party auditors (TPAs) perform functions of data audit conducted in the cloud, thereby safeguarding information access. This auditing human controls the cloud - based data despite how handled their assets are, including through distributing nature. This means the data owner is involved in a way other than providing information in the TPA scheme. In case the TPA marks up any particular group of information, a notice is immediately sent to an owner who can check everything using audit logs and make sure that changes were made [14]. Moreover, every data owner is free to re - audit any time they feel that something has gone wrong with the data and, in this way, keep continuous surveillance on their information. Alternatively, this approach has its limitations, namely dependency on external communication routes and multiplication of the system vulnerability to medium attack, which would open a portal to a wide range of cyber risks [15].

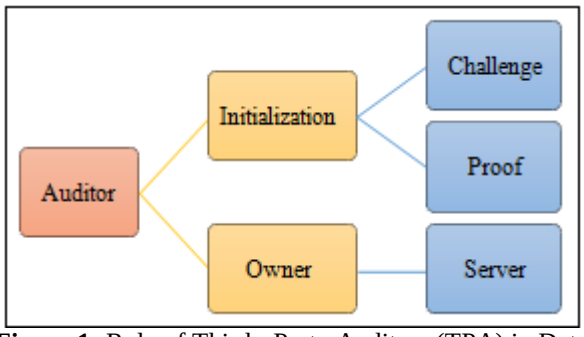

Figure 1: Role of Third - Party Auditors (TPA) in Data Integrity

b) Provable Data Possession (PDP) and Its Variants

Provable data possession (PDP) approach enables the verification of authenticity by downloading only a fraction of dataset. This models the use of probabilistic proofs such as RSA - based homomorphic verifiable tags, allowing clients to verify the ownership of data while not having full access to it. The PDP process starts with the data owners, who change their files with metadata before they upload them to the cloud. After that, integrity verification involves comparing the stored metadata with the data of the cloud server to ensure the data's immutability [16]. Optimized variants of this approach, such as E - PDP, provide better performance, although they need metadata storing at the client's end, which could enlarge the attack surface. In addition, these techniques are not effective for dynamic files such as databases that are constantly updated [1].

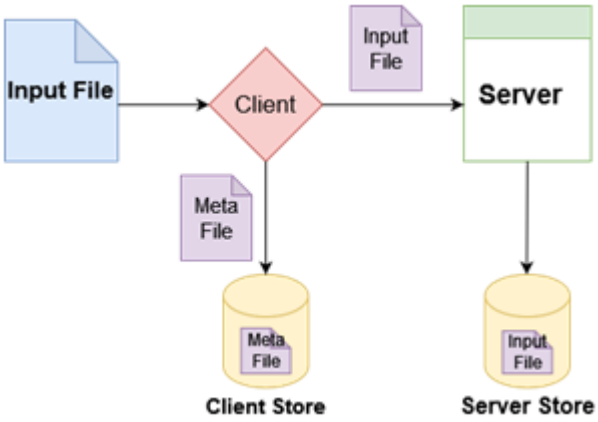

Figure 2: Provable Data Possession (PDP) and Its Variants

c) Blockchain as a Solution for Data Integrity in Cloud Storage

Blockchain technology proposes a new method of ensuring data integrity in cloud storage. Blockchain is a decentralized ledger with blocks containing transaction records. For every block, there is a transaction list and a header with the current and previous blocks' hash. This structure guarantees that all recorded transactions are immutable and verifiable [17]. The decentralized structure of blockchain makes it possible to create a distributed database in which new blocks appear and are checked by network nodes. Blockchain applications also include the recording of file creation, modification, and deletion transactions of both static and dynamic files. For active files, a background process can check for file changes and update hashes at specific intervals. Essentially, blockchain's decentralized structure carries significant minimization of third - party risks and can be seen as a viable option for cloud storage for data integrity [18, 19, 20].

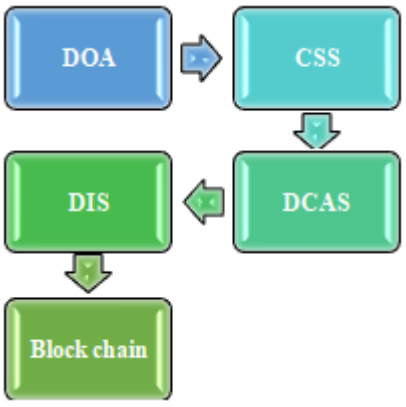

Figure 3: Blockchain as a Solution for Data Integrity

To sum up, despite some benefits that traditional approaches such as TPAs and PDP provide in terms of verifying data integrity, blockchain technology has proved to be much safer and more efficient, which makes it the most desirable option for both dynamic and static data in cloud storage systems [21].

3. System Overview

Our system is bifurcated into two primary components: the front end and the server. The front end, including UI and related programs, interacts with the services of a server. On the other hand, the server must deal with transaction processing and block creation/transmission and is also responsible for user access control [22].

1) Description of the system architecture.

a) **Frontend**: The web application ensures that the UI can be logged into, uploaded from and downloading to its provided storage space for users.

b) **Backend**: The backend, which is the actual core of our system; offers services that are crucial for ensuring file storage integrity. It includes several key elements, such as:

- **ABRAXAS**: This attribute t uses the "File System Watcher" class to watch changes in the file system, spawning and propagating transactions based on such modifications. ABRAXAS makes generalities for transactions differentiated via other filesystem operations like file creation, modification, and deletion.
- **Transaction Processing**: A dedicated worker process then takes these transactions to create blocks, contributing to the blockchain.

2) Details on frontend and backend components of the system

The architecture of contemporary software systems entails frontend components, as well as backend components, each of which contributes significantly to the functionality and the type of user experience [23].

- Client - Server Model**:** There are several systems based on the client - server design, where the server part handles data processing and management. At the same time, the client (or frontend) is targeted at the user interface and data visualization. This model encourages decoupling between parts of the system, and their development and growth can be done separately [24].
- Distributed Architecture**:** One of the other issues, which is becoming a more common trend, is that of the distributed architecture in which the functionalities are divided between a number of systems or modules. This approach also makes it possible to scale, flexibility, and performance enhancement of a system, which is particularly relevant in complex systems such as manufacturing or big data processing [25].

a) Frontend Components

- User Interface**:** The frontend generally encompasses the user interface that developers create using web technologies such as HTML, CSS, and JavaScript. It handles the data of users and also provides data to users as well as capturing user inputs. The interface should be dynamic, intuitive and should quickly and easily process user requests [26].
- Client - side Processing**:** The middleware might require a certain degree of client - side processing, the latter being data validation or even minor data manipulations, to relieve the load from the server connectedness and make the whole process quicker enough for gaining the positive user experience [27].

b) Backend Components

- Data Processing and Management: The backend refers to the central data handling and control stage. It comprises database servers for data storage and retrieval, application servers used to run business logic and APIs, and data interchange mechanisms between the frontend and back end [28].
- Server - side Logic: The server side - logic is complicated by data processing, authentication, authorization and other central logic. It provides data integrity and security, often applying technologies like Python, Node. js, and several database management systems [29].

In summary, system architecture of contemporary software systems is a blend of frontend and the backend attributes. In both sides, the frontend take care of user interface, while the back - end provides the data processing procedures and storage. The segregation makes it easy to build stable, extensible, and efficient systems [30].

Table 1: Features and Applications of Blockchain Technology

Feature	Description	Applications
Scalability	Ability to handle an increasing number of transactions or users	All sectors including finance, healthcare
Real - Time Monitoring	Capability to monitor the chain instantly, using event - based triggers	Security and compliance monitoring
User Isolation	Ensuring individual user activities and data remain separate and secure	Personal data management
Momentary Asset Transfer	Facilitating immediate transfer of assets over the network	Cryptocurrency, digital assets
Immutability	Once recorded, data cannot be altered, ensuring a permanent record	Record keeping, legal documents
Modular Core	Flexibility in modifying and upgrading the system without overhauling the entire architecture	Tech development and adaptation

Table 2: System Components Overview

Component	Description	Key Functions
Frontend	User Interface (UI) and programs for user interaction with cloud storage services.	Access to storage space, uploading/downloading data
Backend	Core system handling data integrity services. Includes components like ABRAXAS and transaction processing units.	Monitoring filesystem changes, processing and creating transactions/blocks

Table 3: Transaction Types in Blockchain System

Transaction Type	Description	Key Attributes
OnCreated	Generated when a new file is created	• Transaction type identifier • Current hash of the file • File path • Digital signature
OnChanged	Triggered when an existing file is modified	• Transaction type identifier • Old and new hash of the file • File path • Digital signature
OnDeleted	Occurs when a file is deleted	• Transaction type identifier • Hash of the deleted file • File path • Digital signature
OnRenamed	Initiated upon renaming a file	• Transaction type identifier • Hash of the file • Old and new file path • Digital signature

These tables constitute a structured and convenient guide to the critical aspects discussed in the paper, ranging from blockchain features to the detailed functions of the system components and transaction types.

4. Model Description

The blockchain model involves specific user - side and server - side functionalities that together underpin the edifice of its well - equipped transaction processing and management system [1].

First, as the user side of the blockchain model, the consumer understands and promises that all information will be public and that they will have perfect recall and consistency of data [2].

1) User Side of the Blockchain Model

- **User Interaction with Blockchain**: Human beings access the blockchain by using digital wallets or client interfaces. The initiated interactions may include transactions, which could be financial, as observed in some cryptocurrencies, and the rest might be related to some other forms of information, such as contracts in smart contracts. As a verification method, the hash code of the user's public key and address information was stored on the blockchain [3, 4, 5].
- **Ensuring Privacy and Security**: It has features through which blockchain ensures user security and privacy. User identifiers are cryptographically based, keeping privacy and safeguarding their activities with the help of digital keys. They are also cryptographically signed where they are crosschecked over the network, and this also ensures that the privacy and security of the transactions are ubiquitous [6].

2) Server Side of the Blockchain Model

- **Distributed Ledger Technology**: The back end includes keeping the ledger of the blockchain distributed among various nodes. Each node is the representation of a blockchain and also serves to validate transactions and read to record. It supports this democratic aspect, which is not based on an actual government that strengthens the data integrity and security within the blockchain [7].
- **Transaction Validation and Consensus Mechanism**: The hash functions such as PoW or PoS are used to authenticate the transactions. All such means make it possible to provide that the entry, kept in a respective ledger, meets some imposed criteria; this list of necessary characteristics does not include any fraudulent transactions and ensures integrity. These mechanisms have the provision that miners or validators are critical elements within their operations, which effectively validate transactions and produce new chain blocks [8].

3) Transaction Processing and Management in Blockchain

- **Transaction Lifecycle**: A transaction stage is decomposable into stages like initiation, validation expansion, and confirmation. In each transaction, each node must broadcast the message regarding the transaction so that it can receive verification as part of the node transaction. Once approved based on consensus, such a transaction can be a part of the new block. When a block is added to the chain, the transaction is confirmed and cannot be reversed [9].
- **Efficient and Secure Transaction Management**: Blockchain uses a number of tools to facilitate the handling of transactions effectively and safely. Most cryptographic methods are used to protect the transaction data and give a timestamp, and the consensus algorithm is used to make all nodes agree upon the state of the ledger. Other innovations, such as smart contracts, help to automate selected steps of processing transactions, relying on automatic execution according to the pre - defined rules [10].

The blockchain model offers an exotic collection of functions, user - side as well as server - side. Still, primarily, they guarantee the safety of the managed and transferred amount of money and the high level of transparency provided by default [11]. The average user interacts with the blockchain through a wallet and clients, starting and authenticating transactions. On the part of the server here, a dotted network of nodes committee validates and records these transactions, keeping the rampancy of the blockchain ledger intact and secure [12]. The lifecycle of blockchain - based transaction processing and management involves the stages of transaction instantiation, transaction validation, block creation, and confirmation, with cryptographic security and consensus algorithms supporting the process. This general interface lets blockchain provide secure and efficient transactions in different applications [13].

5. Blockchain and Data Integrity

1) The concept of blockchain as a distributed database.

As a distributed database, blockchain technology becomes essential in maintaining data integrity and protecting it from illegal changes. Through cryptographic mechanisms and reinforced with consensus algorithms, it can most effectively prevent data tampering as well as enable safe means of digital transactions, plus maintaining secure computerized records [14]. Its application is still receiving widespread acceptance in fields where data integrity has to be

maintained, and the facilities include the healthcare sector and financial industry [15]. Data storage and data management in industries are changing significantly with the present - day trends due to the widespread use of blockchain technology. This tech lies in data integrity and security through no one, as well as safety with an inability to fix [16].

2) The role of blockchain in ensuring data integrity and security

Blockchain is a form of distributed ledger that operates on top of a decentralized network. Compared with the related concept, blocks of data are submitted and connected by means of much more complex cryptography. This is the reason why it serves as one of the most practical solutions in spheres like healthcare, where data safety defines its functioning [17]. Blockchain can be utilized for the management of medical records, and this will assist in ensuring that there is integrity as well as data security [18]. It is guaranteed that data cannot be counterfeited in the cryptography application. In addition, it is a cost - efficient and manageable system that is blockchain - based, and patient records become veer located in various medical institutions.

Consensus algorithms provide the bulk of blockchain function. They also ensure that the network is secure and trustful as they validate transactions and data integrity from end to end into all systems. The main attribute of the blockchain is that it cannot be tampered with. Its architecture, relying on cryptographic hash functions and decentralization, makes it impossible to tamper with data that was uploaded into the blockchain so as to maintain the verifiability of goods [19, 20].

To continue the improvement of data security in blockchain - supported decentralized cloud environments, advanced technologies like the Shuffle Standard Onetime Padding Encryption (S2OPE) have emerged. These developments seek to enhance secured data storage in such environments. These improvements play a crucial role in enhancing the integrity and security of the data, especially in decentralized scenarios, since these predetermined encryption methods may only sometimes be sufficient [21].

The adoption of blockchain technology, especially in the sense of distributed databases, is one of the most substantial steps taken to date to ensure data authenticity and safety. Its architecture, which works as a decentralized system, has the support of useful encryption and consensus mechanisms, and it makes blockchain an excellent solution for the industries that require it to meet the need for high data security and integrity [22].

6. Challenges in Cloud Data Integrity

Cloud integrity is also infected with numerous challenges in the current digital world because the digital entity prefers cloud storage to be a basic sub - atom of data control and business administration. Though cloud storage has numerous advantages, such as scalability, convenience, and efficiency, numerous data integrity issues require the cloud to represent robust solutions [12].

1) Issues with data integrity in cloud storage

One of the major problems regarding data integrity of storage data on the cloud is the setting of data on a failure of function of equipment, bugs of software, and interference because of invasion of the attacker. Here, the openness of the cloud - based storage model, along with the fact that power is often handed over to third - party providers, adds more layers of complexity and risks. It results in doubts about the integrity and consistency of data archived in the cloud. As such, a large number of companies still need to be ready to use a cloud storage solution fully, leading to the fact that people still prefer the old approach of storage that offers more safety and control [23].

2) Traditional methods of ensuring data integrity

In cloud computing platforms, the traditional approaches to preserving data integrity include cryptographic solutions and policy - guided enforcement. Data is protected and secured using encryption, with cryptography facilitating this act in an irreplaceable manner by making sure that only the desired person can access the information without our authorization; the data cannot be changed or altered in any manner, whether it is during transmission to ending or while in store. Methods such as encryption, hash, and digital signature are prevalently employed for protecting data integrity [24]. Indeed, these approaches are enough only in cloud computing as cloud infrastructures have a high level of complexity and scale. Besides, liability - based security enforcement, which has so far proved beneficial in traditional distributed architectures, may be limited in the cloud, where control over the applications and server access is often outsourced to third - party suppliers. Therefore, where the success of policy enforcement is thwarted, data integrity assurance becomes a daunting task [25].

To cope with cloud storage's specificities, different approaches should be developed that are based on the conventional routine activities methods. Such cryptographic protocols are the ones better in line with cloud environment, and also building on advanced data validity verifications like Proof of Retrievability (PoR) or Provable Data Possession (PDP). These operations allow efficient and secure data integrity verification without the need to get all information from their cloud, offering a realistic approach for obtaining honesty in such systems of memory units [26, 27, 28].

The challenges associated with data integrity in cloud storage are caused by what happens inside the clouds. Therefore, to fight these issues more advanced security mechanisms and tools linked with the cloud should be used. Secondly, policies for the development of cloud technology that are aimed at ensuring accuracy and consistency in data stored on the cloud should also be highly emphasized [29, 30].

6.1 Integration of Blockchain with Cloud Storage

1) Integration process of blockchain with cloud storage

Cloud data integrity is one of the major issues that are related to clouds which can be addressed by integration blockchain technology with cloud storage. Through cryptographic mechanisms and reinforced with consensus algorithms, it can most effectively prevent data tampering as

well as enable safe means of digital transactions, plus maintaining secure computerized records. Its application is still receiving widespread acceptance in fields where data integrity has to be maintained, and the facilities include the healthcare sector and financial industry [5].

2) How blockchain technology addresses the challenges in cloud data integrity

Data storage and data management in industries are changing significantly with the present - day trends due to the widespread use of blockchain technology. This tech lies in data integrity and security through no one, as well as safety with an inability to fix [8, 10].

Blockchain is a form of distributed ledger that operates on top of a decentralized network. Compared with the related concept, blocks of data are submitted and connected by means of much more complex cryptography. This is the reason why it serves as one of the most practical solutions in spheres like healthcare, where data safety defines its functioning. Blockchain can be utilized for the management of medical records, and this will assist in ensuring that there is integrity as well as data security. It is guaranteed that data cannot be counterfeited in the cryptography application. In addition, it is a cost - efficient and manageable system that is blockchain - based, and patient records become more available in various medical institutions [12, 15, 19].

Consensus algorithms provide the bulk of blockchain function. They also ensure that the network is secure and trustful as they validate transactions and data integrity from end to end into all systems. The main attribute of the blockchain is that it cannot be tampered with. Its architecture, relying on cryptographic hash functions and decentralization, makes it impossible to tamper with data that was uploaded into the blockchain so as to maintain the verifiability of goods. This process of integration also typically necessitates customizing existing cloud - storage infrastructure to facilitate blockchain technology and its inherent protocols and algorithms that are compatible with operating blockchain activities [20].

Specifically, challenges that are faced on the issue of cloud data integrity are being dealt with by the inbuilt properties of blockchain technology. This, first of all, allows the distributed character of blockchain to be provided, thus removing the number of single points of failure and improving the overall security level and robustness of the cloud storage system [3]. For such a network, where data is distributed across a system of nodes, it is always possible for the partners to control the whole set differently, reducing the danger of data modification by one node and the loss of the entire volume of data due to the failure of a node [5, 6]. Second, since the network's data is immutable once it is placed in the blockchain, the data would need a consensus of the network to alter it. This capability is critical in securing data integrity because every data transaction, including input - output, undertaken within the cloud storage system becomes permanent, immutable, and transparent. Furthermore, blockchain uses sophisticated cryptographic mechanisms to secure data to ensure that data cannot be tampered with or leaked to unauthorized parties [7, 13].

Therefore, is that forcing blockchain and cloud storage integration is a significant evolution of basing the problem of cloud data integrity. By nature, blockchain technology is decentralized, immutable, and secure; therefore, it is a robust solution to increase the security, transparency, and dependability of cloud storage systems. This technology will likely continue to evolve, playing an increasingly important role in molding the future of cloud data management and security systems [18, 25].

6.2 Utilizing blockchain for ensuring the integrity and traceability of sensitive data

1) Different approaches and protocols in blockchain for data integrity

Utilizing blockchain technology for ensuring the integrity and traceability of sensitive data offers numerous advantages due to its inherent characteristics. Here's an overview of how blockchain can be applied to safeguard sensitive data [2, 4, 9]:

a) **Immutable Ledger**: One of the core features of blockchain is its ability to create an immutable ledger of transactions or records. The data stored on the blockchain is immutable and tamperproof, thus it can't be removed or changed. Such permanence and safety of information guarantee inviolability and security [1].
b) **Decentralization**: It is most prominent of the features where blockchain will be working only within a network of nodes instead of traditional databases. Based on this design and attachment with the smart contract, it does not maintain any centralized location that may be exposed to the threat of failure or breaches. If there is compromise in one node, he data in all other nodes will help in progress an unharmed and authorized way of implementation [29].
c) **Encryption and Security**: Data on the blockchain is typically encrypted, which adds an additional layer of security. Blockchain technology incorporates cryptographic features to safeguard data from unauthorized entry [2].
d) **Traceability and Transparency**: Every recorded transaction or document in blockchains is timestamped and associated, thus maintaining traceability and transparency. An auditable trail which could be subjected to open verification for information validation and to track back any changes, access and transactions of sensitive data to the source is created [5].
e) **Smart Contracts**: Such smart contracts support automated processes or transactions that are defined based upon pre - specified rules. The blockchain networks, for example, the Ethereum platform, utilize these platforms in order to limit tampering and human error risks that may emerge from human involvement in managing data as well as dealing with sensitive information [8].
f) **Access Control**: Access control in a blockchain can be enforced to limit data access only for the authorized users of private keys. This will make the data confidential, which are meeting up the privacy laws as approval would be needed in order to have access to selective data within a blockchain [11].
g) **Interoperability and Data Exchange**: Blockchains integrate data exchange capabilities, making the data to be transferable even in other systems or blockchains, yet

safely. This will greatly benefit trades like health, especially when sharing patient - related information on multiple platforms with a number of players [22].

h) **Regulatory Compliance**: Regulatory Compliance Relatively, Blockchain technology can provide an acceptable alternative / remedy for employment in industries that mostly need to comply with very strict rules for the protection of data imposed on them by law. For instance, auditable and tamper - proof data that is being stored on a blockchain has the potential to allow organizations to fulfill their respective data integrity as well as reporting - related regulations [3, 6].

Organizations, businesses, and companies can, therefore, further their data security together with the storage and management of critical as well as sensitive information with the deployment of blockchain technology [23]. Besides integrity and traceability functionalities that come as an appendage within the integration, all the rigorous requirements of security and the necessary ones in compliance would have been passed through [23].

2) Methods and techniques used in blockchain to ensure data integrity

a) Blockchain technology uses different approaches and techniques to confirm data integrity in all forms. Such methods define the basis for the maintenance of data privacy in blockchain systems [5].

b) **Cryptographic Hash Functions**: Cryptographic hashing is one of the basic approaches necessary to preserve the data integrity in the blockchain [6, 30]. All the blocks in a blockchain are represented with a unique hash – a cryptographic fingerprint – that is created from the content of the block. 'Any change made to the data will change this hash, thus signifying a break in the data integrity. In this case, this method is suitable for verifiable end - to - end systems that include blockchain - based e - voting, secure data exchange applications, and others [1].

c) **Data Auditing**: This transformation is brought about by blockchain applications in enterprise information systems. Through the incorporation of blockchain, periodic audits of databases can be conducted in a decentralized environment, thus ensuring data integrity without depending on a database that is centralized entirely [2].

d) **Blockchain - Based Data Integrity Verification**: The Data Integrity Service framework based on blockchain technology ensures that data integrity can be verified reliably and securely without assistance from TPAs. This framework is more effective in dynamic environments that are dynamic such as IoT, where traditional TP - A - based frameworks do not act reliably [3].

e) **Decentralized and Public Auditing Protocols**: Hash chaining is a method that integrity audits preserving decentralization do besides it has an ability to be used in smart contracts and open verifications as well due to blockchain realization. These protocols get rid of the need for a central TPA and permit auditing abilities & transparency to go public. More precisely, they utilize immutability and non - repudiation as the two faulty characteristics of blockchain to replace all manual - based processes with technologies depending on this concept [4].

f) **Identity - Based Encryption and Blockchain**: Blockchain with identity - based encryption increases the security of data. This corresponds to what happens by combining both encryption elements that ensure the protection of user data and identity and prevent both identity thefts and fraud. It provides a secure data storage platform and ensure user privacy is kept intact [5].

g) **Data Integrity Scheme for IoT**: As far as these bilinear design techniques to maintain data integrity based on blockchain are concerned, they are designed by focusing on the application of IoT data. Blockchain technologies are used in such schemes to provide data integrity, which helps to overcome the issues of traditional approaches where TPAs are involved and play an important role [6].

The blockchain system combines the ledger distributed by technology with advanced cryptographic methods, which helps to ensure robust and efficient data authenticity solutions. These approaches not only improve a system's security but also add some transparency to the way data is managed and decentralized [7, 8].

6.3 Applications of blockchain in maintaining a secure and unforgeable audit trail for Private/government services

Blockchain technology has attracted a lot of attention from different sectors because it is endowed with many features and benefits. In particular, it offers scalability and chain monitoring in real - time with event - driven triggers used to separate users and immediate transfer over the network of assets without an immutability modular core [9]. These properties make blockchain technology very well suited to file monitoring, a vital process in information security. Blockchain technology must be addressed in the provision of reliable, sensitive data integrity and traceability across different sectors. Some blockchain use cases for keeping a consistent, immutable audit trail for private and public services in various industries include the following [10, 11]:

1) Healthcare Sector:

- **Patient Data Management**: Blockchain technology can be used to produce an indelible concatenation of patients' medical history in a way that entries cannot be changed, edited, or modified. This makes it a reliable source of information regarding patients for healthcare practitioners [12].
- **Drug Traceability**: Blockchain technology performs tracking of drug manufacturing, supply chain architecture and delivery. This helps to combat counterfeit medicine and preserve quality medication [13].

2) Financial Services:

- **Transaction Auditing**: In the banking and finance industry, blockchain acts as an irreversible ledger of transactions that translates into greater transparency and security. It may also eliminate and certify insurance claims that reduce fraud [14].
- **Smart Contracts in Insurance**: Smart contracts available through blockchain make automated processing and verifying of insurance claims possible according to

predefined parameters reducing the possibilities for fraud [15].

3) Government Services:

- **Voting Systems**: The implementation of blockchain in the voting systems provides a guarantee for the integrity of elections as it represents a transparent, auditable, and anonymous nature. It might also serve as an archive for public documents such as land records, and birth certificates that can be securely stored [16, 17].
- **Public Records**: Various other public documents, such as land registries and birth and death certificates, can use blockchain to take an archive of him so that he can authenticate the same [18, 19, 20]

4) Supply Chain Management:

- **Product Traceability**: Blockchain technology allows tracking a product's lifecycle from the manufacturing stage through to reselling, so as to demonstrate its provenance and legitimacy. It also ensures the needs of supply chain regulation [21].
- **Compliance Tracking**: It also allows compliance with the regulated regulatory requirements for products across its entire development cycle order to keep high standards and ethical business practices [22].

5) Energy Sector:

Grid Management and Energy Trading: The energy grid can be efficiently managed by blockchain, especially in the case of distributed energy resources such as solar panel systems using the technology. It facilitates peer - to - peer (P2p) energy trading making possible the sale and purchase of excess power smoothly [23].

6) Education Sector:

Credential Verification: Blockchain can allow for verification of credentials, making it easier to verify documents and reducing the risk associated with fake qualifications [24].

7) Legal Industry:

Document Authentication and Intellectual Property: Verification is reliable for legal documents, contracts, and intellectual property rights as blockchain can authenticate them [25].

In this light, it's important to note that blockchain technology has emerged as a very relevant factor in modern industries, encompassing a host of attributes and benefits that can be transformative in almost all different sectors. Thus, the relevance of blockchain in modern industries has gained traction due to advances in the sector [26, 27]

It is for this reason that this technological advancement is being explored and embraced in different areas of life, such as finance, the healthcare industries, agriculture, education, etc. The usability of blockchain is across a wide range of sectors, including financial sectors, where financial transactions are becoming more efficient, supply chain management, and the healthcare and educational sectors, which benefit from increased data security [28, 29]

The Blockchain facilitates the development of Industry 4.0 and provides solutions for safe, decentralized storage and interactions in IoT networks. Its ban has changed the industrial use of data security, transparency, and efficiency [30]

Blockchain's inherent characteristic is decentralization, which provides better data safety and reduces the risk of security breaches and fraud. This division and elimination are enabled by decentralization, doing away with the need for centralized authorities or mediators in direct transactions and interactions [5, 8, 11].

Within blockchain, data integrity means if data has entered, for instance, it is impossible to change without altering the whole chain. The non - changing nature of blockchain that ensures that it is clear to anybody who wants to verify or examine the data allows all the participants to be able to check and deny data from where there is a need to inflict defiance due to its nature on end each of different users [15, 17, 20].

On the one hand, smart contracts in blockchain replace the intermediary parties and automate enforcement and contract terms, thus making transactions both efficient and secure. What makes this feature especially valuable is that it is helpful in the financial, legal, and real estate professions [21, 24].

Blockchain technology is highly applicable in modern industries due to its flexibility and the fact that it provides safe, transparent, and decentralized solutions. It is changing both business and individual behavior as it becomes integrated into different sectors, which enables more efficient, secure, and decent practices [25, 28]

These examples illustrate the usage of blockchain technology in different fields, which ensures that a secure and immutable audit trail is maintained, thereby increasing transparency, security, and efficiency while handling sensitive data [1, 9, 30].

7. Conclusion

In conclusion, Blockchain technology has become popular in recent times because it ensures data integrity and security. This study identified the Clark and Wilson model which is one of the well - known security model can be combined with blockchain technology in order to make sure the integrity of data. The Clark and Wilson model looks at the concept of integrity, characterized as the accuracy and consistency in data. It determines a collection of rules and constraints that must be applied to preserve the integrity of data. All these rules are separation of duties, well - formed transactions, and certification individuals. These rules and controls can be enforced by blockchain technology. Blockchain is a form of distributed and decentralized ledger. It uses a safe and transparent recording system to keep transaction records. Every transaction is included in a block that gets appended to the previous one, forming chains. This enables information integrity because the data cannot be changed. Under this integrative approach, the Clark and Wilson model is incorporated with blockchain technology so

that organizations are better able to preserve data integrity. The model is a guide for how to create and maintain rules, and blockchain technology ensures the security of transactions. This union is especially instrumental in sectors that require data integrity, including finance, health, and supply chain management. Blockchain technology, interestingly, possesses a unique set of features that enable it to promote the integrity of data. However, the very essence of blockchain is a decentralized, distributed, and shared ledger that records transactions in a decentralized network environment, making it highly resilient against unauthorized change:

1) Decentralization**:** The Peer - To - Peer (P2P) nature of the blockchain removes the central points of failure, which has a great impact on the risk of data tampering and loss. It is the decentralization of data that guarantees that intelligence is not under the clutches of one body, which in turn ensures the integration of data.
2) Immutability**:** As soon as a transaction has been entered into the blockchain through its entry, it has been branded literally unsusceptible to the change of not only its notation but also its deletion from the blockchain. This immortality is indispensable in the endeavor to achieve data authenticity and dependability to be stored.
3) Cryptography**:** Blockchain uses complex cryptographic mechanisms to secure transactions and data, which prevents information from being accessed illegally and makes it impossible for any breaches to occur.

References

[1] S. Aldossary and W. Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions, " International Journal of Advanced Computer Science and Applications, vol.7, no.4, 2016. [Online]. Available: https: //pdfs. semanticscholar. org/09fd/5326be429b39d75103ddd6550176c10e0ba3. pdf

[2] G. Ateniese et al., "Provable Data Possession at Untrusted Stores, " in Proceedings of the 14th ACM conference on Computer and Communications Security, pp.598 - 609, October 2007. [Online]. Available: https: //dl. acm. org/doi/abs/10.1145/1315245.1315318

[3] I. Zikratov et al., "Ensuring Data Integrity Using Blockchain Technology, " in 2017 20th Conference of Open Innovations Association (FRUCT), pp.534 - 539, April 2017. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/8071359/

[4] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk A Blockchain - Based Decentralized File Storage Application, " Storj Labs Inc., Technical Report, 2014. [Online]. Available: https: //storj. io/metadisk. pdf

[5] Y. Sompolinsky and A. Zohar, "Secure High - Rate Transaction Processing in Bitcoin, " in Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26 - 30, 2015, Revised Selected Papers, pp.507 - 527, 2015. [Online]. Available: https: //link. springer. com/chapter/10.1007/978 - 3 - 662 - 47854 - 7_32

[6] D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies, " in 1987 IEEE Symposium on Security and Privacy, pp.184 - 184, April 1987. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/6234890/

[7] S. Nakamoto, "Bitcoin: A Peer - To - Peer Electronic Cash System, " Bitcoin, 2008. [Online]. Available: https: //www.klausnordby. com/bitcoin/Bitcoin_Whitepaper_Document_HD. pdf

[8] G. Zyskind and O. Nathan, "Decentralizing Privacy: Using Blockchain to Protect Personal Data, " in 2015 IEEE Security and Privacy Workshops, pp.180 - 184, May 2015. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/7163223/

[9] A. Majot and R. Yampolskiy, "Global Catastrophic Risk and Security Implications of Quantum Computers, " Futures, vol.72, pp.17 - 26, 2015.

[10] I. Zikratov et al., "Ensuring Data Integrity Using Blockchain Technology, " in 2017 20th Conference of Open Innovations Association (FRUCT), pp.534 - 539, April 2017. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/8071359/

[11] R. Kalis and A. Belloum, "Validating Data Integrity with Blockchain, " in 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp.272 - 277, December 2018, [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/8591029/

[12] C. Machado and A. A. M. Fröhlich, "IoT Data Integrity Verification for Cyber - Physical Systems Using Blockchain, " in 2018 IEEE 21st International Symposium on Real - Time Distributed Computing (ISORC), pp.83 - 90, May 2018. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/8421150/

[13] R. Anascavage and N. Davis, "Blockchain Technology: A Literature Review, " SSRN 3173406, 2018. [Online]. Available: https: //papers. ssrn. com/sol3/papers. cfm?abstract_id=3173406

[14] H. Wang and J. Zhang, "Blockchain Based Data Integrity Verification for Large - Scale Iot Data, " IEEE Access, vol.7, pp.164996 - 165006, 2019. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/8895808/

[15] O. Firica, "Blockchain Technology: Promises and Realities of The Year 2017, " Calitatea, vol.18, no. S3, p.51, 2017. [Online]. Available: https: //search. proquest. com/openview/63ea3fd6602715d854ef11bac09236b6/ 1?pq - origsite=gscholar&cbl=1046413

[16] J. Wu et al., "Cloud Storage as The Infrastructure of Cloud Computing, " in 2010 International Conference on Intelligent Computing and Cognitive Informatics, pp.380 - 383, June 2010. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/5565955/

[17] I. Arora and A. Gupta, "Cloud Databases: A Paradigm Shift in Databases, " International Journal of Computer Science Issues (IJCSI), vol.9, no.4, p.77, 2012.

[18] O. Marian, "Are Cryptocurrencies Super Tax Havens?, " Mich. L. Rev. First Impressions, vol.112, 2013, p.38.

[19] A. F. Skarmeta, J. L. Hernandez - Ramos, and M. V. Moreno, "A Decentralized Approach for Security and Privacy Challenges on The Internet of Things, " in 2014 IEEE World Forum on Internet of Things (WF - IoT), pp.67 - 72, March 2014. [Online]. Available:

https: //ieeexplore. ieee. org/abstract/document/6803122/
[20] Z. K. Zhang, M. C. Y. Cho, and S. Shieh, "Emerging Security Threats and Countermeasures in Iot, " in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp.1 - 6, April 2015. [Online]. Available: https: //dl. acm. org/doi/abs/10.1145/2714576.2737091
[21] D. R. Stinson, "Some Observations on The Theory of Cryptographic Hash Functions, " Designs, Codes and Cryptography, vol.38, pp.259 - 277, 2006. [Online]. Available: https: //link. springer. com/article/10.1007/s10623 - 005 - 6344 - y
[22] M. G. Karpovsky, L. B. Levitin, and A. Trachtenberg, "Data Verification and Reconciliation with Generalized Error - Control Codes, " IEEE Transactions on Information Theory, vol.49, no.7, pp.1788 - 1793, 2003. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/1207376/
[23] D. Burger et al., "Scaling to the End of Silicon with EDGE Architectures, " Computer, vol.37, no.7, pp.44 - 55, 2004. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/1310240/
[24] J. Madhavan et al., "Web - Scale Data Integration: You Can Only Afford to Pay as You Go, " Google Research, 2007. [Online]. Available: https: //research. google/pubs/pub32784/
[25] A. Halevy, A. Rajaraman, and J. Ordille, "Data Integration: The Teenage Years, " in Proceedings of the 32nd International Conference on Very Large Databases, pp.9 - 16, September 2006. [Online]. Available: https: //www.cin. ufpe. br/~if696/referencias/integracao/_Data_Integration - The_Teenage_Years. pdf
[26] B. Y. Reis et al., "AEGIS: A Robust and Scalable Real - Time Public Health Surveillance System, " Journal of the American Medical Informatics Association, vol.14, no.5, pp.581 - 588, 2007. [Online]. Available: https: //academic. oup. com/jamia/article - abstract/14/5/581/720868
[27] U. Dayal et al., "Data Integration Flows for Business Intelligence, " in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology, pp.1 - 11, March 2009. [Online]. Available: https: //dl. acm. org/doi/abs/10.1145/1516360.1516362
[28] E. E. Schadt et al., "Computational Solutions to Large - Scale Data Management and Analysis, " Nature Reviews Genetics, vol.11, no.9, pp.647 - 657, 2010. [Online]. Available: https: //www.nature. com/articles/nrg2857
[29] C. Gütl et al., "Adele (Adaptive E - Learning with Eye - Tracking): Theoretical Background, System Architecture and Application Scenarios, " European Journal of Open, Distance and E - Learning, vol.8, no.2, 2005. [Online]. Available: https: //old. eurodl. org/?p=archives&year=2005&halfyear=2&article=197
[30] H. Yan et al., "BGPmon: A Real - Time, Scalable, Extensible Monitoring System, " in 2009 Cybersecurity Applications & Technology Conference for Homeland Security, pp.212 - 223, March 2009. [Online]. Available: https: //ieeexplore. ieee. org/abstract/document/4804446/