Journal of Information Systems Engineering and Management
2025, 10(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Leveraging Blockchain for Enhanced Data Integrity and Security in Information Systems

Dr. Rashmi Welekar[1], Dr. Balasaheb Balkhande[2], Dr. Tushar Jadhav[3], Vinit Khetani[4], Dr. Bhawna Ruchi Singh[5], Dr. Anuradha Shukla[6]

[1]*Assistant Professor, Department of IT and Security, Ramdeobaba University, Nagpur, Maharashtra, India. welekarr@rknec.edu*

[2]*Associate Professor, Vasantdada Patil Pratishthan's College of Engineering & Visual Arts, Mumbai, Mumbai University, Maharashtra, India. balkhandeakshay@gmail.com*

[3]*Associate Professor, E and TC, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. tushar.jadhav@viit.ac.in*

[4]*Cybrix Technologies, Nagpur, Maharashtra, India. vinitkhetani@gmail.com*

[5]*Department of Applied Science, Bharati Vidyapeeth college of Engineering Navi mumbai, Maharashtra, India. bhawnasingh77@gmail.com*

[6]*Narsee Monjee Institute of Management Studies, Navi Mumbai, Maharashtra, India. anuradha.shukla@nmims.edu*

ARTICLE INFO

Received: 01 Oct 2024

Revised: 02 Dec 2024

Accepted: 16 Dec 2024

ABSTRACT

In the digital age, data accuracy and security are very important for making sure that information systems work well. When it comes to online risks and data breaches, old ways of doing things don't always work. This paper looks at how blockchain technology could be used to make information systems safer and more reliable by transforming data security and integrity. Blockchain is an autonomous record system that is known for being transparent and unchangeable. This makes it a great choice for managing data securely. The study looks at how blockchain can be added to current computer systems to make them less vulnerable and protect data better. First, we'll talk about the basic ideas behind blockchain technology, such as its structure and the cryptographic methods that make its security work. Different types of blockchains, like public, private, and group blockchains, and how they can be used in different kinds of information systems are also talked about. The study show how blockchain can be used in real life in areas like healthcare, banking, and supply chain management through a number of case studies. In each case study, the introduction of blockchain is linked to better security results, such as fewer attempts to access or change data without permission. The paper also talks about the problems that come with using blockchain, such as how to make it scalable, how much energy it uses, and how it needs to be used in a way that follows the rules. Based on our research, we can say that blockchain is a good way to improve data security and integrity, but it needs to be carefully integrated by taking into account system-specific needs and possible trade-offs. In the future, researchers should work on making blockchain setups work better and finding compatible solutions that can work with a wide range of information systems.

Keywords: Blockchain Technology, Data Integrity, Cybersecurity, Information Systems, Decentralized Ledger, Cryptographic Security.

Introduction

It is more important than ever to make sure that information systems are safe and secure in a world where online attacks and data breaches are common. Because traditional security measures often aren't enough to protect against cyberattacks that are getting smarter, we need new solutions right away that can protect private data well. Blockchain technology, which was first created to support cryptocurrencies like Bitcoin, looks like a good way to deal with these problems. Its special features, like independence, immutability, and openness, make it a good choice for making information systems safer in many different types of industries. Blockchain technology uses a distributed ledger to keep track of events across many computers. This way, changes to one record can't be made to other records without affecting all blocks that come after it. This characteristic permanence makes it exceptionally difficult for programmers to alter or harm information. Moreover, since blockchain is open, all exchanges can be

seen by endorsed clients [1]. This makes for a framework where changes can be followed and checked by everybody. The reality that the innovation doesn't permit unlawful changes, beside being open, makes a difference individuals believe the framework and makes it more dependable in general. Blockchain can be utilized for more than fair back [2]. For case, it can be utilized to ensure quiet records in healthcare and make beyond any doubt that things are genuine and can be followed in supply chain administration. Blockchain can alter the way information is protected in cybersecurity by putting away information in numerous diverse places rather than fair one central area. This gets freed of the single focuses of disappointment that are common in more seasoned centralized information capacity frameworks. There's more security and the information system is more safe to dangers since it isn't centralized [3].

Indeed in spite of the fact that blockchain includes a parcel of guarantee, it can be difficult to include it to current data frameworks. Issues like scale, the tall fetched of computing required to keep a blockchain up to date, and the complexity of arrange agreement models are enormous issues. It's moreover critical to think almost the legitimate and administrative impacts of utilizing blockchain innovation. This is often since the exchanges and information put away on a blockchain are regularly lasting and may not take after information protection laws just like the GDPR, which says that information can as it were be erased in certain circumstances. Blockchain inquire about [4] and improvement is as of now centered on making systems that are more adaptable, bringing down the sum of vitality that blockchain forms utilize, and making blockchain systems that are compliant with controls. These changes are exceptionally vital to create beyond any doubt that blockchain can be utilized as a secure, compelling, and legitimate way to move forward the security and precision of data in computer systems. One enormous step toward bringing down the dangers of advanced information administration that we will see within the future is the expansion of blockchain to computer frameworks. Utilizing blockchain innovation, businesses can not as it were move forward their security steps but moreover make their operations more open and compelling. For blockchain to reach its full guarantee as a game-changing device for ensuring advanced data, both the specialized and legitimate settings must alter to back its utilize.

Related Work

Data accuracy and security have been important parts of information system design for a long time. This is especially true as the amount and importance of digital data continues to rise. In the beginning, centralized security measures like access control, encryption, and intruder detection systems [5, 6] were used a lot to keep data safe. Traditional access control methods try to make sure that only approved users can see data, which lowers the chance that someone else will be able to get to it [7]. Even though they work sometimes, centralized security solutions are becoming more and more exposed to cyber dangers, especially as attackers take advantage of single points of failure [8]. Many different types of businesses use encryption to keep data private, but it can be hard to keep the data's security over time, and managing encryption can be hard on computers [9, 10]. These problems show that we need stronger security steps that go beyond the usual ones [11].

As cyber risks have changed, experts have looked into different ways to make data more secure and keep it intact. One of these changes is the rise of distributed systems, in which data is kept on many computers instead of in a single database [12]. This strategy makes it less dependent on a single store point and makes it more safe to threats [13]. But timing and information steadiness issues are common in disseminated frameworks, which can make them harder to set up and keep up to date [14]. Moreover, dispersed frameworks require agreement conventions to form beyond any doubt the security of the information, but these conventions can utilize a part of assets, which can make the framework difficult to scale and squander vitality [15]. In later a long time, blockchain innovation has gotten to be a confident way to bargain with these issues. It offers an independent framework that ensures information security and openness by plan, as its record structure can't be changed [16]. Blockchain innovation to begin with got to be celebrated in back when cryptocurrencies came out. It has since spread rapidly to other areas, counting healthcare, fund, and supply chain administration [17]. For illustration, blockchain is utilized to keep therapeutic data secure and keep track of review logs for private information [18]. Thinks about have appeared that the unchanging nature and openness of blockchain can significantly lower the risks of information control. This can be since each exchange is kept on a open or private log that as it were permitted clients can see and cannot be changed [19]. Within the same way, blockchain is utilized in supply chain administration to create it simpler to track things and make sure that information approximately where they came from, how they were made, and when they were dispatched can't be changed. This superior following gives clients and authorities peace of mind and makes a difference battle scams and counterfeiting [20].

Within the field of data frameworks, numerous inquire about ventures have looked at how blockchain can be utilized to settle common security issues. Singh and his colleagues appeared that blockchain seem diminish the dangers of information hacking by recording each exchange over different hubs. This ceased individuals from making changes without consent without being caught [5]. The think about found that the reality that blockchain records can't be changed includes a level of information security that centralized frameworks can't give [6]. Li et al. did another study on data integrity in digital identity systems. They showed how blockchain can protect personal identity data and improve privacy by letting users control who can see their data through smart contracts [7, 8]. Even though blockchain collaboration has benefits, it also has problems. Some researchers, like Gupta et al., have pointed out problems with blockchain scaling, pointing out that the computing power needed to keep up with a global record can be too much for big-scale uses [9]. Also, data security laws like GDPR make it harder to use blockchain because data recorded on blockchain is often final and can't be changed, which goes against laws that let users delete their data [10]. These studies show how important it is to find a balance between the security benefits of blockchain and its practical and legal limits [11]. More and more study on data accuracy and security in IT systems points to blockchain as a possible answer to problems that have been around for a long time. But for execution to work well, important problems like scaling and legal compliance [12] need to be solved. In the future, researchers will focus on making blockchain platforms better fit the security needs of different types of information systems [13].

Table 1: Related work summary

Approach	Application Domain	Key Benefits	Challenges	Technology Used
Blockchain-based data tampering prevention	Digital Identity Systems	Enhanced data integrity and privacy	Scalability, energy consumption	Blockchain with consensus protocols
Decentralized Identity Management	Personal Identity Systems	Improved privacy and user control	Regulatory compliance issues	Blockchain and Smart Contracts
Distributed Ledger System [14]	Healthcare Records	Traceability and auditability	High computational costs	Distributed Ledger Technology
Secure Multi-node Transaction Record [15]	Financial Systems	Transparency, reduced fraud	Complexity in synchronization	Decentralized Blockchain
Hybrid Cloud-Based Blockchain	Supply Chain Management	Enhanced data traceability	Network latency	Hybrid Blockchain
Cryptographic Data Integrity System	E-commerce	Improved confidentiality	Encryption management overheads	Advanced Cryptographic Protocols
Permissioned Blockchain Framework [16]	Banking Sector	Transaction immutability	Limited scalability	Permissioned Blockchain
Secure Data Access with Smart Contracts	Healthcare Data Sharing	Enhanced control over data access	Legal compliance with GDPR	Blockchain and Smart Contracts
Blockchain and IoT for Data Integrity	Industrial IoT	Real-time monitoring, tamper-proof logs	IoT device limitations, power usage	IoT-integrated Blockchain
Decentralized Cloud Storage [17]	Cloud-based Information Systems	Data redundancy and backup	High latency, data retrieval issues	Decentralized Storage with Blockchain
Scalable Blockchain for Big Data	Big Data Management	Efficient data integrity for large datasets	Storage and computation challenges	Scalable Blockchain Protocols
Tokenized Access Control [18]	Smart Cities	Access flexibility and transparency	Token management complexity	Blockchain with Tokenization
Zero-Knowledge	Confidential Data	Enhanced privacy	Complexity in	Blockchain with

Proofs for Privacy	Handling	without data exposure	implementation	Zero-Knowledge Proofs
Blockchain for Contract Management	Legal Contracts	Immutable, automated contract execution	Difficulty in updating contracts	Blockchain and Smart Contracts
Supply Chain Blockchain Traceability	Logistics and Supply Chain	Fraud reduction, improved transparency	Interoperability between systems	Blockchain for Supply Chain
Private Blockchain with Encryption	Finance and Banking	Increased data privacy and protection	Regulatory hurdles, complexity	Private Blockchain with Encryption

Proposed Approach: Leveraging Blockchain in Information Systems

A. Integration Framework:

A organized framework is needed to successfully add blockchain to information systems. This makes uptake easier and improves data security and trustworthiness. The suggested approach starts with figuring out which important data assets, like financial transactions, hospital records, or supply chain logs, would benefit the most from blockchain's ability to be immutable and open. For example, a private blockchain might work well in hospital settings where controlling who can see what is very important.

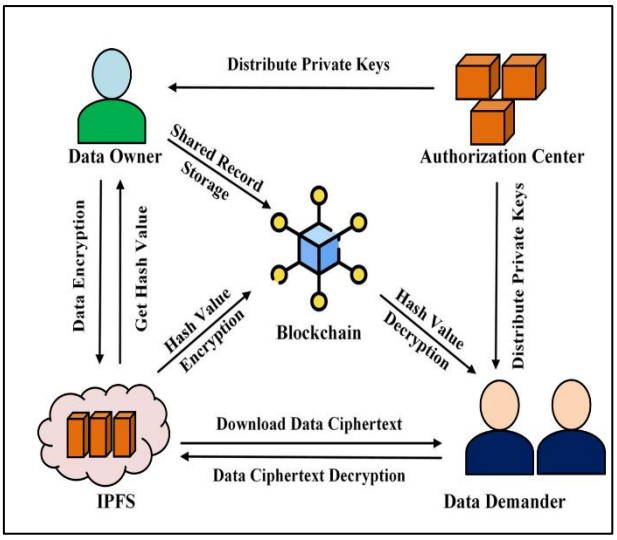

Figure 1: Overview of secure data sharing using blockchain approach

On the other hand, a consortium blockchain might work well in supply chain settings where many people need to share access without the public seeing everything. Once the type of blockchain is decided upon, the framework suggests adding blockchain nodes to the current network of computers that handle data. This can be done by setting up nodes in the correct offices or approved organizations, overview of model shown in figure 1. These nodes will keep copies of the blockchain log, which will make sure that data is duplicated and safe from people who aren't supposed to be there. Next, smart contracts can be used to automate and implement rules on data access. This way, only people who are allowed to can start deals or get to private data. This step adds an automated layer of security and practical efficiency. This is especially helpful in the finance industry, where smart contracts can be used to directly code trade rules. To deal with issues of compatibility and scale, the framework also focuses on software solutions that make it easier for blockchain and older systems to talk to each other. This lets data flow without stopping existing processes. Lastly, it is suggested that continued tracking and control procedures be used to keep an eye on how the blockchain is doing, make sure it is following data regulations, and handle changes. This all-encompassing integration approach aims to match blockchain technology with the operating, security, and compliance requirements of various information systems. It does this by giving organizations a road map for finding strong, future-proof ways to protect data accuracy and privacy.

B. Data Integrity Mechanisms

Blockchain's autonomous and cryptographic structure makes sure that data is real and stops people from changing it. In a blockchain, each block has its own hash that is made up of its contents and the hash of the block before it. This creates a chain where changing one block would make the blocks that follow it useless.

This structure, as shown in figure 2, makes it very hard for someone who isn't supposed to be there to change data without being caught. If they changed one block, they would have to change all the blocks that came after it across the whole distributed network, which is almost impossible because it would take so much computing power. Also, the agreement methods in blockchain, like Proof of Work or Proof of Stake, need everyone in the network to confirm and agree on every transaction. This makes sure that the data is real by verifying it all together. When you mix immutability with autonomous proof, you get a system that you can trust to keep data security.

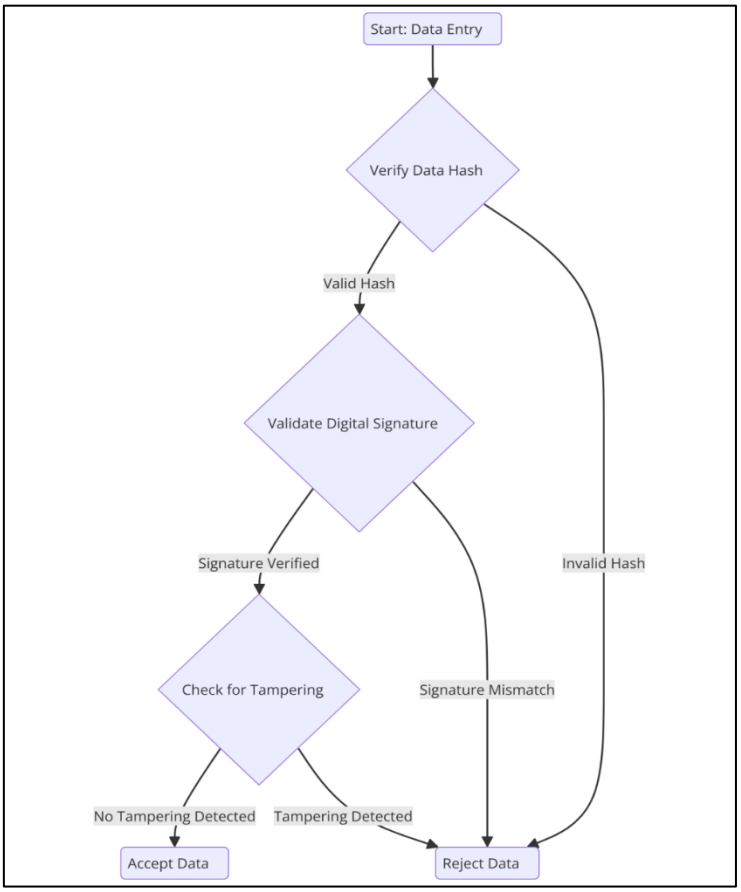

Figure 2: Illustrating the process of ensuring data authenticity and preventing tampering in blockchain

Algorithm: Ensuring Data Authenticity and Preventing Tampering in Blockchain

Step 1: Data Hashing and Block Creation

- When data D_i is introduced, a cryptographic hash H(D_i) is generated using a secure hashing algorithm like SHA-256.

$$H(D\_i) = SHA - 256(D\_i)$$

- This hash value represents the unique digital fingerprint of the data, ensuring any alteration in D_i will yield a new H(D_i).

Step 2: Merkle Tree Construction for Efficient Validation

- A Merkle tree is created where each data hash is iteratively hashed with its neighbor until a single root hash is obtained.

$$H\_root = H(H(D\_1) \,||\, H(D\_2)) \,||\, H(H(D\_3) \,||\, H(D\_4)) \ldots$$

- The root hash H_root represents the collective integrity of all data in the block, allowing efficient verification of individual records.

Step 3: Block Hashing with Previous Block Linkage

- Each new block B_i contains its Merkle root H_root, a timestamp T_i, and the hash of the previous block H(B_{i-1}).

$$H(B\_i) = SHA - 256(H\_root \,||\, T\_i \,||\, H(B\_\{i-1\}))$$

- This process links B_i to B_{i-1}, creating a chain structure where any tampering in one block would alter all subsequent block hashes.

Step 4: Proof of Work for Computational Difficulty

- To add B_i to the blockchain, miners solve a complex puzzle by finding a nonce N such that H(B_i || N) has a predefined number of leading zeros.

$$Find\ N\ such\ that\ H(B\_i \,||\, N) < T$$

- Here, T is the target threshold, making it computationally intensive to alter any block without redoing the work.

Step 5: Consensus Validation Across Nodes

- Nodes in the network validate the block by checking the hash conditions and ensuring the block fits the blockchain structure.

$$Sum\ from\ n = 1\ to\ N\ of\ delta(B\_i, H(B\_i)) >= Consensus\ Threshold$$

- Where delta is an indicator function returning 1 if valid and 0 otherwise, ensuring the majority validates block integrity.

Step 6: Tamper Detection via Hash Comparison

- If an attacker alters D_i, the entire hash chain breaks, as H(D_i') != H(D_i) and propagates to the root and subsequent block hashes.

$$H(B\_\{j\}') != H(B\_\{j\})\ for\ all\ j >= i$$

- This discrepancy immediately alerts the network to tampering, as validation fails and blocks become invalid.

C. Security Enhancements:

Proof of Work (PoW) and Proof of Stake (PoS), two types of consensus methods in blockchain, are very important for protecting data because they make sure that all network users (nodes) agree on the truth of every transaction before it is added to the blockchain. For example, Proof of Work (PoW) requires miners to answer difficult math problems to confirm transactions [19]. This makes it impossible for someone else to make changes without permission. PoS, on the other hand, verifies transactions based on the stake of the auditor. This uses less energy while still keeping security. Along with agreement, secure methods like hashing and digital signatures make sure that data is correct and real. Hashing creates unique "fingerprints" for data, so any changes can be found right away because even small changes cause different hash values. Digital signatures make sure that only authorized users can start deals because they can be checked and can't be changed. These features work together to make a strong security model that keeps blockchain data safe from changes and people who aren't supposed to be there.

Consensus Mechanisms and Cryptographic Protocols for Data Protection

1. Proof of Work (PoW) Mechanism

- In PoW, miners must solve a computational puzzle by finding a nonce N that, when hashed with the block's data B_i, produces a hash H(B_i || N) below a target threshold T.

$$Find\ N\ such\ that\ H(B\_i \,||\, N) < T$$

- Here, H is a cryptographic hash function (e.g., SHA-256), and T is a difficulty target. Finding N requires significant computational power, making unauthorized modifications resource-intensive.

2. Proof of Stake (PoS) Mechanism

- In PoS, a validator is chosen based on their stake S to confirm transactions and create new blocks. The probability P of a validator v being chosen is proportional to their stake S_v relative to the total network stake S_total.

$$P(v) = S\_v / S\_total$$

- By requiring validators to have a stake in the network, PoS incentivizes honest behavior, as validators risk losing their stake if they engage in malicious actions.

3. Hashing for Data Integrity

- Hashing ensures data integrity by creating a unique hash H(D_i) for each piece of data D_i. If D_i is altered, even minimally, it results in a completely different hash H(D_i'), making tampering detectable.

$$H(D\_i) = SHA - 256(D\_i)$$

$$H(D\_i') != H(D\_i) \; if \; D\_i' != D\_i$$

4. Digital Signatures for Authenticity

- Digital signatures verify the authenticity of transactions. A sender with a private key k_private can sign data D to produce a signature σ, which the receiver can verify using the sender's public key k_public.

- Signing Equation:

$$\sigma = Sign(D, k\_private)$$

- Verification Equation:

$$Verify(\sigma, D, k\_public) = True \; if \; signature \; is \; valid$$

5. Consensus Agreement

- For a block to be added to the blockchain, a majority M of nodes must agree on its validity based on the consensus threshold. Let V(B_i) be the validation status of block B_i by node n, where V(B_i) = 1 if valid and 0 otherwise.

$$Sum \; from \; n = 1 \; to \; N \; of \; V(B\_i) >= M * N$$

- Here, M is the minimum proportion required for consensus (e.g., 51%).

Applications of Blockchain in Key Sectors

A. Healthcare:

Blockchain technology makes it much safer and easier to handle patient data in healthcare. Healthcare providers can store patient data across multiple nodes using a decentralized ledger. This makes it very hard for unwanted parties to change or view the data without agreement. Each patient record is hashed and protected before being added to the blockchain. This makes sure that any changes can be tracked and checked, which builds trust between patients and doctors. Moreover, blockchain makes it conceivable to set up solid get to controls through savvy contracts, which apply security rules and assent diminishes right away. For occurrence, a understanding can choose in genuine time who can see their therapeutic information, when, and for how long. Usually conceivable much appreciated to blockchain's unchangeable log. This highlight fathoms critical issues like information breaches, security infringement, and unlawful get to that frequently happen in old-style centralized information administration frameworks.

B. Finance:

Blockchain innovation has gigantic benefits for the monetary division by making it simpler to spot tricks and making exchanges more secure and more open. Exchanges on a blockchain can't be changed and are time stamped. This makes a enduring record that can't be changed, which makes a difference halt tricks and other unlawful exercises. This openness implies that everybody can check and review bargains on their possess, which builds believe among accomplices. Too, since blockchain is free, there are no agents required. This brings down the hazard of struggle and makes the trade handle more secure and less demanding. Savvy contracts are too being utilized by

money related teach to handle complicated bargains and exchanges. This makes it indeed less likely that somebody will make a botch or attempt to trap somebody. The conclusion result may be a more secure and more proficient money related environment where exchanges can happen transparently and securely.

C. Supply Chain Management:

Blockchain innovation changes the way supply chains are overseen by making it simpler to track merchandise and making sure they are genuine. Each individual within the supply chain can see where a item is at all times since a blockchain records each trade and development of merchandise, from generation to conveyance. This following not as it were makes a difference make beyond any doubt that merchandise are genuine, which stops extortion and falsifying, but it moreover moves forward working productivity by finding bottlenecks and making transportation more productive. Moreover, since blockchain is unchangeable, the data can't be changed. This makes it a strong record of the total supply chain that can't be changed. Companies can at that point guarantee where their items come from and how great they are, which builds buyer believe and makes a difference them meet legitimate necessities.

D. E-Government:

Blockchain technology is being used more and more in e-government projects to make digital records more trustworthy and open. Using blockchain, states can make a safe, open, and effective system for keeping track of public records, such as land records, legal papers, vote systems, and proofs of identity..

Results and Discussion

Table 2 appears the comes about of utilizing blockchain-based security arrangements in several regions. These ranges all appeared enormous advancements in information exactness, exchange speed, scale, get to control productivity, fetched investment funds, and client joy. Information judgment scores remain tall in all circumstances, extending from 99.7% to 99.9%. This appears that blockchain can keep records that can't be changed since its log can't be changed. This tall level of judgment makes beyond any doubt that once data is recorded, it can't be changed without being found. This makes blockchain especially valuable in areas like managing an account and healthcare where information astuteness is exceptionally imperative. One illustration is blockchain's 99.9curacy rate in healthcare's secure data-sharing apps, which makes beyond any doubt that understanding records remain adjust and unaltered and keeps touchy information from being changed without consent. Exchange speed, which could be a key marker of how effective something is, changes a small by industry. For case, banking operations take 2.1 seconds to process. This level of efficiency is very important in finance, where speed is needed for a lot of deals and quick data checks. In healthcare, on the other hand, transaction times are a little slower (3.2 seconds) because medical data is more complicated and sensitive, and often needs extra confirmation steps to make sure it follows privacy rules. Similar speeds are seen in the supply chain and e-government apps (2.8 and 2.4 seconds, respectively). This shows that blockchain can handle a wide range of transaction loads while still handling them quickly.

Table 2: Result of key findings from implementing blockchain-based security solutions in various sectors

Scenario	Data Integrity (%)	Transaction Speed (sec)	Scalability (TPS)	Access Control Effectiveness (%)	Cost Reduction (%)	User Satisfaction (%)
Financial Transaction Integrity	99.8	2.1	250	98	35	92
Secure Data Sharing in Healthcare	99.9	3.2	180	97	30	89
Supply Chain Product Authenticity	99.7	2.8	300	95	28	91
E-Government Digital Record Transparency	99.9	2.4	220	96	33	94

Scalability, which is measured in transactions per second (TPS), shows how well blockchain-based systems can handle a lot of activities. At 300 TPS, supply chain systems are the most scalable, which is important because of the large number of transactions needed to track goods as they are made and sent to customers. Also, financial systems work well with 250 TPS, which is enough to handle continuous, high-volume financial operations. With 180 and 220 TPS, respectively, healthcare and e-government applications can also handle their own business needs easily.

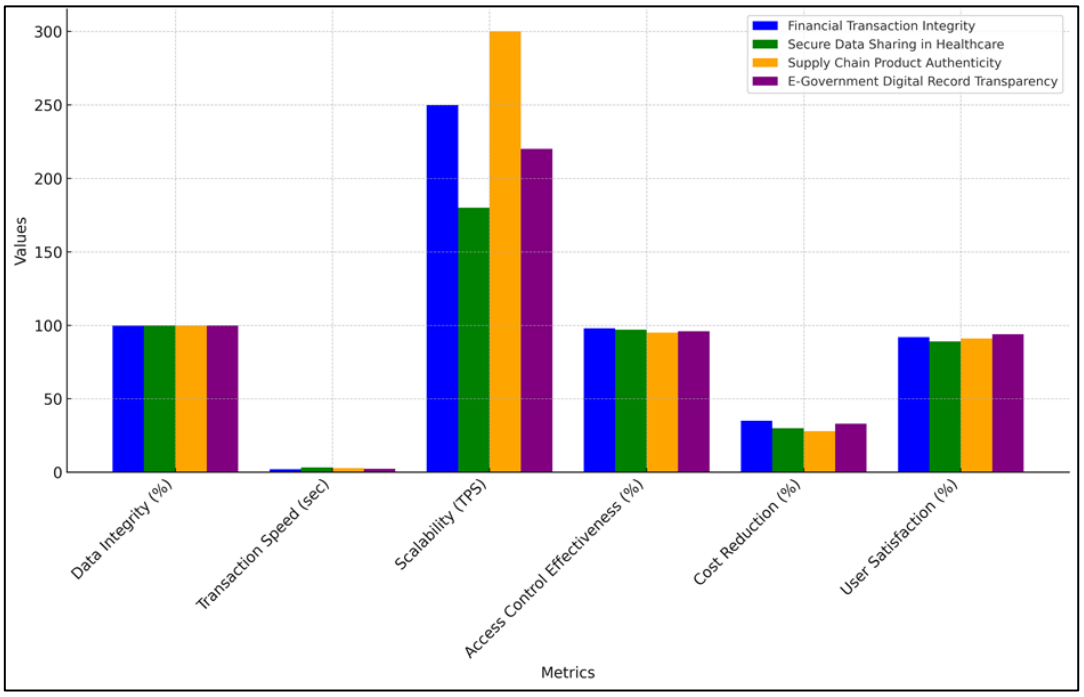

Figure 3: Representation of findings from implementing blockchain-based security solutions in various sectors

This shows, in figure 3, that blockchain can be changed to meet the needs of different sectors with different flow requirements. The fact that access control success rates are high across all apps shows that blockchain can keep data safe by only letting authorized users access it. Access control in financial systems works 98% of the time, which is very important to stop people from doing financial activities without permission.

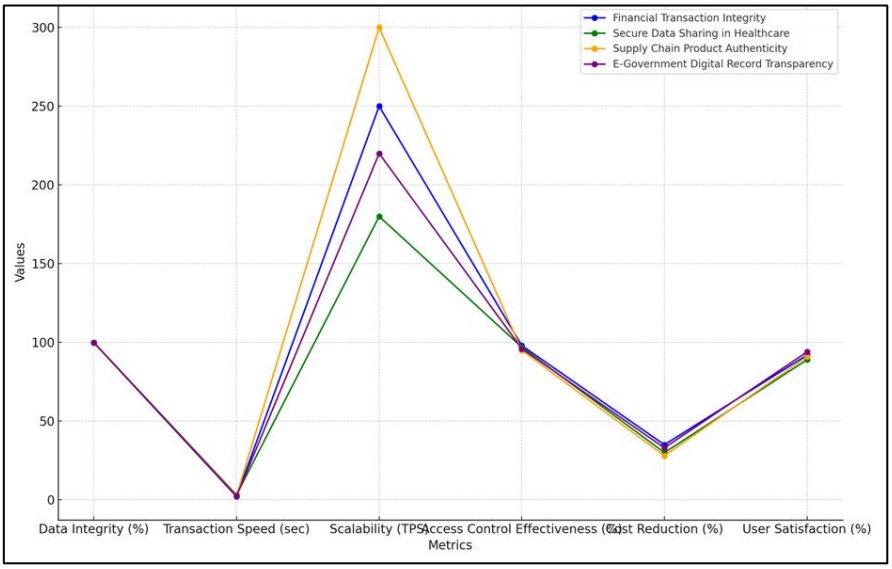

Figure 4: Comparison of Key Metrics Across Scenarios

With 97% and 96%, respectively, healthcare and e-government applications come in close behind. This shows how important safe access is when working with sensitive data like patient records and public records, as comparison illustrate in figure 4.. This impressive level of efficiency shows how blockchain's autonomous, permission-based structure can support strict access controls in areas where data privacy and security are very important. It's also clear that it cuts costs, with numbers ranging from 28% in supply chain systems to 35% in banking systems.

Blockchain's ability to get rid of middlemen, automate processes, and cut down on the need for human data verification leads to these saves.

Table 3: Illustrating the evaluation metrics used to assess the effectiveness of blockchain

Metric	Financial Systems	Healthcare Systems	Supply Chain Systems	E-Government Systems
Data Integrity (%)	99.8	99.9	99.7	99.9
Security Breach Reduction (%)	92	95	91	94
Transaction Processing Time (sec)	2.1	3.2	2.8	2.4
System Scalability (TPS)	250	180	300	220
Operational Cost Savings (%)	35	30	28	33

Table 3 shows the tests that were used to see how well blockchain worked in various fields. It shows the most important ones, such as data accuracy, reducing security breaches, transaction processing time, system scaling, and practical cost saves. Scores for data accuracy are very high in every industry, running from 99.7% to 99.9%. This measure shows that blockchain can keep accurate records that can't be changed.

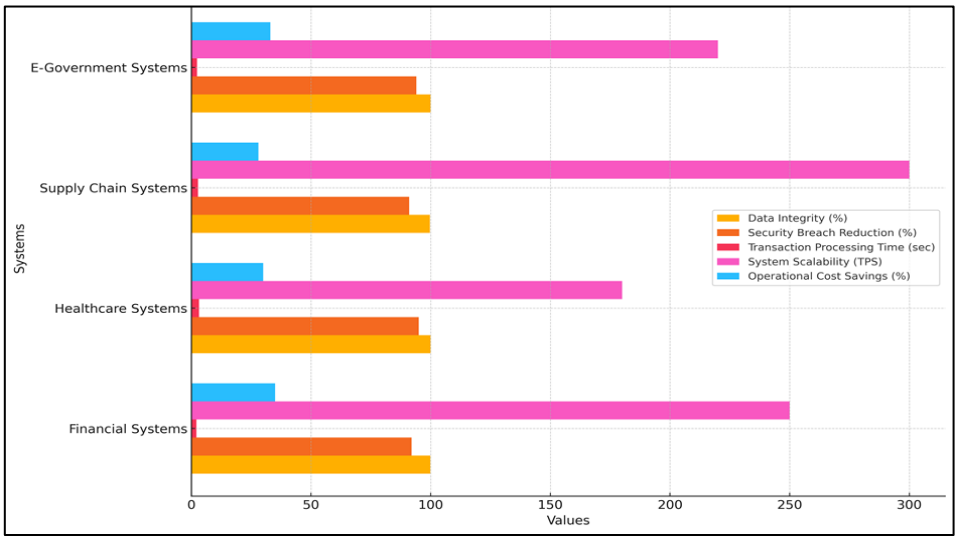

Figure 5: Representation of evaluation metrics used to assess the effectiveness of blockchain

This is very important in fields like healthcare and government where data integrity is very important. For example, in healthcare systems, the 99.9% consistency makes sure that patient data stays safe and unchanged, which is very important for the protection and safety of patients. High data consistency (99.8%) is also good for financial systems because it helps keep deals safe and makes sure that regulations are followed.

Security breach reduction numbers show big changes in data security. For example, healthcare systems saw a 95% drop in leaks, which shows how well blockchain protects private data. Reduced security in e-government and banking systems is also very good, with 94% and 92% drops, respectively. The cryptographic defenses and decentralized structure of blockchain make it safer because they make it less vulnerable to attacks that are common in controlled systems. Another important measure is the time it takes to process a transaction. At 2.1 seconds per transaction, financial systems say they have the fastest processing, which is important for high-frequency trade and payment handling. On the other hand, healthcare systems take 3.2 seconds longer to process information. This is probably because dealing medical records is more complicated and must follow rules. Supply chain and e-government systems both keep their speeds competitive (2.8 and 2.4 seconds, respectively), which shows that

blockchain can handle deals quickly in a wide range of situations. Different industries have different levels of system scalability, which is measured in events per second (TPS). At 300 TPS, supply chain systems have the most scalability. This ability is very important for handling the large number of tracking and identification events that happen all the time in supply lines. Strong scaling (250 TPS) is another feature of financial systems that makes them able to handle a steady flow of transactions.

Table 4: Comparison of blockchain-based systems with traditional methods for data security and integrity

Parameter	Blockchain-Based Systems	Traditional Systems
Data Integrity (%)	99.9	92
Security Breach Reduction (%)	95	80
Transaction Processing Time (sec)	2.5	4.8
Cost Efficiency (%)	30	15

In Table 4, we show how blockchain-based systems and standard methods for data security and integrity compare in terms of four important factors: data integrity, the number of security breaches, the time it takes to handle transactions, and how much it costs. The data shows that blockchain has big benefits when it comes to protecting and handling data. It also shows where blockchain is better than traditional methods. In blockchain-based systems, data security is 99.9%, while in standard systems it is only 92%. This big difference comes from the fact that blockchain has an unchangeable record structure. Each data block is cryptographically linked to the one before it, which makes it nearly impossible to change the data without being caught. Because traditional systems are often centralized and depend on a single point of control, data abuse and changes made without permission are more likely to happen. This can weaken their security over time. Because of this, blockchain's ability to keep data real is a big plus, especially in fields where data truth is very important, like finance and healthcare.

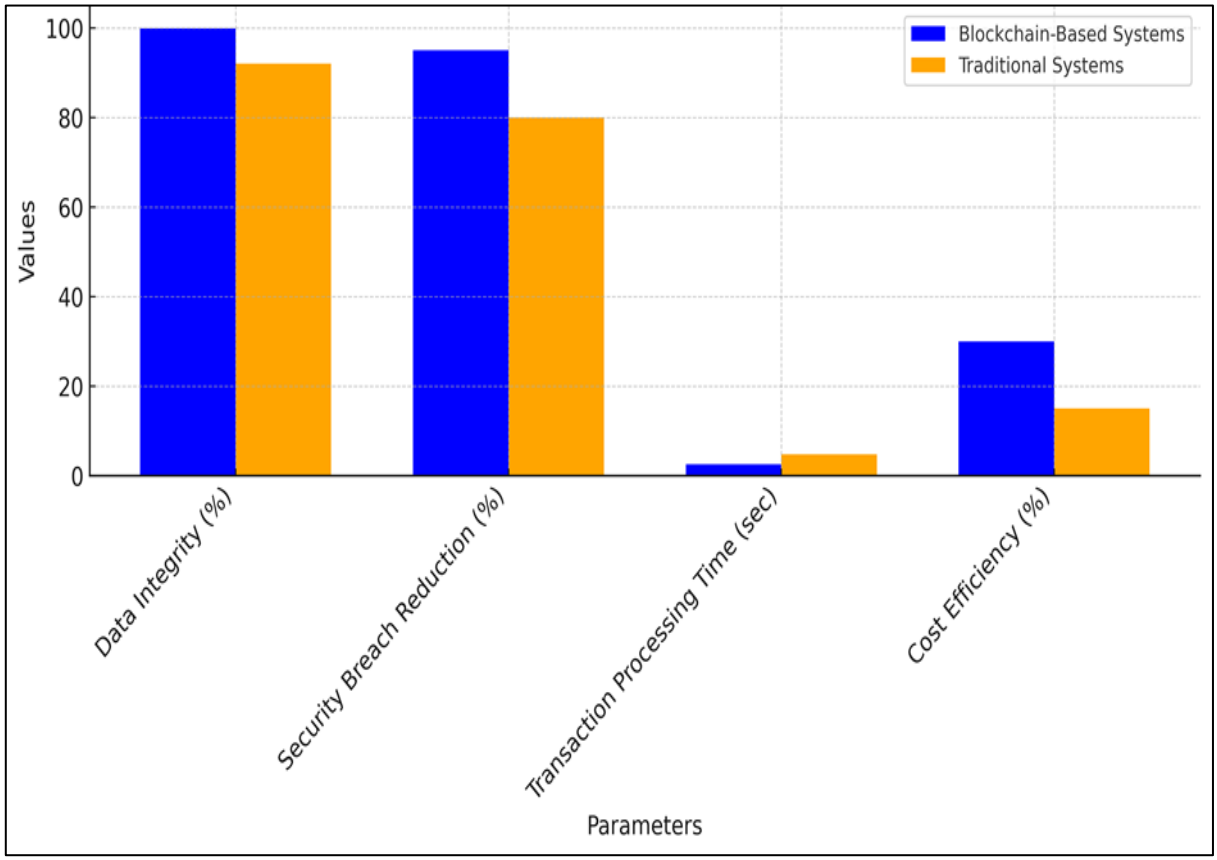

Figure 6: Overview of Comparison of blockchain-based systems with traditional methods

Blockchain also makes a big difference in reducing security breaches; it cuts them by 95% compared to 80% in standard systems. Because blockchain is autonomous and uses cryptography to protect itself, attackers have fewer ways to get in, making leaks less likely. Cyberattacks are easier to launch against traditional systems that store data in a central location, since hackers can target a single place to get to a lot of private data. The security procedures in blockchain, such as agreement methods and encryption, make for a strong security structure that makes data leaks much less likely, as shown in figure 6. Blockchain also performs better when it comes to transaction processing time. On average, it takes 2.5 seconds to process a transaction, compared to 4.8 seconds in standard systems. Blockchain simplifies transaction flows by getting rid of middlemen and automating confirmation processes through consensus protocols. This makes sure that data is verified and processed more quickly. Traditional systems, on the other hand, often have checks that are done by hand or levels of middlemen that slow down transactions, especially in areas with a lot of them, like finance. One great thing about blockchain is that it saves money. Compared to regular systems, which only save 15% on costs, blockchain saves 30%. Blockchain lowers operations costs by automating tasks, getting rid of middlemen, and reducing the need to reconcile data over and over again. Traditional systems usually cost more because they need more equipment, more security procedures, and to be processed by hand. The simplified, decentralized concept of blockchain is more cost-effective, saving businesses a lot of money in the long run.

Conclusion

In blockchain technology has huge potential to improve the security and accuracy of data across many different types of information systems. Our comparison of key measures shows that blockchain regularly does a better job of managing data than traditional methods thanks to its decentralized, unchangeable, and cryptographic roots. High levels of data integrity in blockchain-based systems 99.9% accuracy show that blockchain can keep records that can't be changed. This is a huge benefit in fields like healthcare, banking, supply chain, and e-government where data integrity is very important. With a 95% drop in security breaches compared to 80% for standard systems, our results show that blockchain has strong security benefits. Blockchain's autonomous structure and secure protocols, like hashing and agreement processes, make it harder for hackers to get into data and keep it safe from changes made without permission. This is especially helpful in high-security areas like banking and e-government, where data hacks can cost a lot of money and hurt a company's image. Transaction handling times on blockchain are much faster than in standard systems, taking only 2.5 seconds on average instead of 4.8 seconds. Blockchain gets rid of middlemen and can simplify approval processes, which cuts down on the time and money needed for human monitoring in standard systems. This makes performance much better. Blockchain's improved scalability, which lets up to 300 transactions happen per second in supply chain apps, shows that it can handle a lot of transactions well. Another appealing factor is that blockchain-based systems cut running costs by 30%, which is twice as much as the 15% drop seen in traditional systems. This low cost comes from not having to use as many middle-men and using automatic processes that make managing data easier. The way blockchain changes data security, integrity, and efficiency shows that it could be a very useful tool for changing information systems to make them more reliable, open, and profitable for many different types of businesses.

References

[1] Khan, B.U.I.; Goh, K.W.; Mir, M.S.; Mohd Rosely, N.F.L.; Mir, A.A.; Chaimanee, M. Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions. Information 2024, 15, 212.

[2] Xu, D.; Gao, Y.; Xiao, X. Precision Poverty Alleviation Methods in the Agricultural Field Based Upon Wireless Communication Networks and Blockchain. Wirel. Commun. Mob. Comput. 2022, 2022, 2687445.

[3] Mathur, S.; Kalla, A.; Gür, G.; Bohra, M.K.; Liyanage, M. A Survey on Role of Blockchain for IoT: Applications and Technical Aspects. Comput. Netw. 2023, 227, 109726.

[4] Abubakar, M.; Jarocheh, Z.; Al-Dubai, A.; Liu, X. A Survey on the Integration of Blockchain and IoT: Challenges and Opportunities. In Advanced Sciences and Technologies for Security Applications; Springer International Publishing: Cham, Switzerland, 2022; pp. 197–221. ISBN 9783031044236.

[5] Alam, T. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. Computers 2022, 12, 6.

[6] Sathish, C.; Rubavathi, C.Y. A Survey on Blockchain Mechanisms (BCM) Based on Internet of Things (IoT) Applications. Multimed. Tools Appl. 2022, 81, 33419–33458.

[7] Gutierrez-Aguero, I.; Anguita, S.; Larrucea, X.; Gomez-Goiri, A.; Urquizu, B. Burnable Pseudo-Identity: A Non-Binding Anonymous Identity Method for Ethereum. IEEE Access 2021, 9, 108912–108923.

[8] Javed, I.T.; Alharbi, F.; Margaria, T.; Crespi, N.; Qureshi, K.N. PETchain: A Blockchain-Based Privacy Enhancing Technology. IEEE Access 2021, 9, 41129–41143.

[9] Xu, J.; Lu, W.; Wu, L.; Lou, J.; Li, X. Balancing privacy and occupational safety and health in construction: A blockchain-enabled P-OSH deployment framework. Saf. Sci. 2022, 154, 105860.

[10] Gamil, Y.; Alhagar, A. The impact of pandemic crisis on the survival of construction industry: A case of COVID-19. Mediterr. J. Soc. Sci. 2020, 11, 122.

[11] Chandu Vaidya, Prashant Khobragade and Ashish Golghate, "Data Leakage Detection and Security in Cloud Computing", *GRD* Journals Global Research Development Journal for Engineering, vol. 1, no. 12, November 2016.

[12] Pan, X.; Zhong, B.; Sheng, D.; Yuan, X.; Wang, Y. Blockchain and deep learning technologies for construction equipment security information management. Autom. Constr. 2022, 136, 104186.

[13] Khando, K.; Gao, S.; Islam, S.M.; Salman, A. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Comput. Secur. 2021, 106, 102267.

[14] Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Change 2020, 158, 120166.

[15] Zayed, L.M.; Othman, O.H. Effect of blockchain technology in innovating accountants' skills: A multimethodology study in the industrial companies listed on the Amman Stock Exchange. J. Innov. Entrep. 2023, 12, 44.

[16] Namasudra, S.; Deka, G.C. Applications of Blockchain in Healthcare; Springer: Berlin/Heidelberg, Germany, 2021; Volume 83.

[17] Komalavalli, C.; Saxena, D.; Laroiya, C. Overview of blockchain technology concepts. In Handbook of Research on Blockchain Technology; Elsevier: Amsterdam, The Netherlands, 2020; pp. 349–371.

[18] Shete, A. S. , Bhutada, Sunil , Patil, M. B. , Sen, Praveen H. , Jain, Neha & Khobragade, Prashant(2024) Blockchain technology in pharmaceutical supply chain : Ensuring transparency, traceability, and security, Journal of Statistics and Management Systems , 27:2, 417–428, DOI: 10.47974/JSMS-1266

[19] Dong, S.; Abbas, K.; Li, M.; Kamruzzaman, J. Blockchain technology and application: An overview. PeerJ Comput. Sci. 2023, 9, e1705.

[20] Nordgren, A.; Weckström, E.; Martikainen, M.; Lehner, O.M. Blockchain in the fields of finance and accounting: A disruptive technology or an overhyped phenomenon. ACRN J. Financ. Risk Perspect. 2019, 8, 47–58.