***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

Integrating Blockchain with Cloud-Based Relational Databases for Decentralized Data Integrity and Enhanced Security

Uday Kumar Manne[1]
[1]Database Engineer, Adobe Inc
udaykumarmanne@gmail.com[1]

Amit Goswami[2]
[2]Software Developer, Source Infotech
amitbspp123@gmail.com[2]

Hirenkumar Kamleshbhai Mistry[3]
[3]Sr. Linux Admin & Cloud Engineer, Zenosys LLC
hiren_mistry1978@yahoo.com[3]

Chirag Mavani[4]
[4]DevOps / Cybersecurity Engineer, DXC Technology
chiragmavanii@gmail.com[4]

ABSTRACT:
The swift growth of cloud computing has fundamentally changed the way we process store and manage data. This is primarily because of platforms like Amazon Web Services (AWS) Google Cloud and Microsoft Azure which are well-known for their affordability scalability and flexibility. Even with these developments there are still many obstacles to overcome especially when it comes to protecting data security guaranteeing reliability and avoiding unwanted access—all of which are critical issues in the increasingly digital world where relational databases (RDBs) are essential for effectively connecting and organizing vast amounts of structured data. However issues like data tampering and restricted user control over data are common with traditional centralized systems for managing these databases underscoring the urgent need for creative solutions to improve the security and dependability of cloud-based relational databases. The proposed model uses mobile agent technology to deploy a network of distributed virtual machine agents which serve as the foundation for a blockchain-based system that protects data integrity by carrying out crucial tasks like secure data storage continuous monitoring and real-time verification while also facilitating smooth user collaboration. This study focuses on creating a decentralized system that combines blockchain technology with relational databases hosted in the cloud to improve data security and integrity. By placing a strong emphasis on decentralization security and user-controlled data management this framework not only solves the enduring problems of data integrity and trust in cloud environments but it also offers a safe and effective platform for information management in the quickly evolving digital world of today. It also shows how the combination of blockchain technology and cloud systems can revolutionize data management procedures. Future studies could also concentrate on enhancing this models scalability and computational efficiency which would enable it to be used for a wider variety of cloud computing applications. This would increase the models practical utility and broaden its potential to satisfy the various demands of contemporary cloud-based systems.

Keywords: Big Data Analytics, Machine Learning, Scalability, Decision Making, and Predictive Modeling.

1. INTRODUCTION

With its increased processing power virtual storage and scalable on-demand resources cloud computing has become a game-changing method that is changing how people and organizations use technology in the digital age. Compared to traditional IT systems that depend on a lot of physical hardware and on-site management cloud computing is far more flexible and affordable. By using a metastructure made up of remotely accessible network-enabled components cloud computing allows service providers to effectively manage systems and provide seamless user experiences. The pay-as-you-go model further separates the infrastructure into a virtual layer that users can control and a physical layer that acts as the foundation guaranteeing both operational scalability and financial viability. Relational databases (RDBs) serve as the foundation of cloud platforms by effectively managing structured and connected data while cloud computings distributed storage architecture reduces the risk of data loss through frequent backups making it extremely dependable for modern data management. Leading providers like Google Microsoft and Amazon are creating strong cloud-based RDB products like Google BigQuery Azure SQL Database and Amazon Redshift that support complex queries and ensure high data accessibility. Relational database management systems (RDBMS) add value by guaranteeing consistency and reliability and using Standard Query Language (SQL) to store and retrieve data in tabular formats. Notwithstanding these benefits clients frequently give up direct control over the management and security of their data when storing it in cloud systems which leads to vulnerabilities across several infrastructure layers. As a result the quick growth of cloud computing has spurred significant worries about data security. Since the distributed architecture of cloud metastructures allows data to be stored in any global data center which frequently worries customers about losing control ensuring data safety at every level of the cloud remains a critical challenge. The Cloud Security Alliance (CSA) has identified data loss confidentiality integrity and privacy as major concerns. These risks are significantly increased by centralized management systems where over 60% of data breaches result in large financial losses due to insider threats such as employees abusing their access to compromise sensitive data. As evidenced by numerous applications ranging from safeguarding Internet of Things (IoT) systems to preserving electronic health records blockchain technology with its tamper-proof decentralized framework offers a promising solution by guaranteeing the integrity of cloud data opening the door to a more reliable and secure cloud ecosystem. [1][2]

2. Overview of Decentralized Cloud Computing

Decentralized cloud computing is a big change in cloud services because it moves away from old systems where big companies control and store data on special servers and instead spreads data and work across a network of devices like computers, mobile phones, and servers which helps to make the system safer and stronger by not depending on just one company or server to handle everything so that it reduces problems like data being stolen or systems breaking down too easily. In decentralized cloud computing, there is a thing called peer-to-peer or P2P networks where every device can work as both a server and a client and because data is saved in lots of places it means even if some of the devices stop working, other ones can still give the data that is needed and keep the system running which makes the whole thing more reliable and makes sure people can always get to their data whenever they need it. There are many new platforms making decentralized cloud computing popular, like Golem and iExec, which are used for renting out computing power, and Storj and Filecoin, which are for storing data in a distributed way, and these platforms let people share resources like extra computer space and get paid for it which not only helps save money on building expensive cloud systems but also makes the whole system better for the environment and easier to use for everyone. This way of doing cloud computing has a lot of benefits, like making it harder for data to get lost or stolen, cutting costs, and making the whole system work better, and as shown in figure 1, it is clear that this idea is changing how cloud services are made and used everywhere.

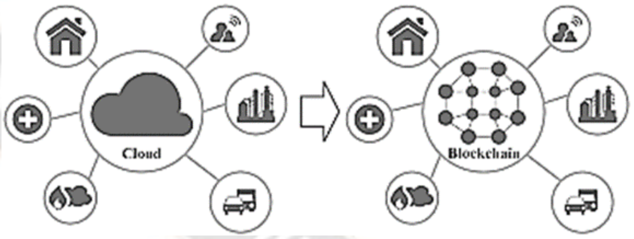

Fig. 1. Decentralized Cloud Computing

Decentralized cloud computing is a big change in how cloud services work because it gives everyone the chance to use and offer cloud services instead of just big companies controlling everything, and this means small businesses and individuals can join the market and compete fairly, which helps to bring more ideas and solutions that fit different needs and encourages people to think of new ways to do things. It also helps with keeping user data private because there is no one big company that can misuse or take advantage of the data, and instead, users can have more control over their own data in a system like this, and it makes sure users don’t have to worry about losing control over what they store. Another big thing about decentralized clouds is that they are very flexible and scalable, which means users can easily make changes or handle more or less work as needed without too much trouble, but even though all these things sound great, there are still some problems like slow speeds, limits on how much data can be sent through networks, and how hard it is to manage systems that are spread out over many places, and these problems have to be fixed before everyone can start using this system.[3][4]

2.1. Importance of Blockchain in Decentralized Systems

Blockchain technology is very important for making decentralized cloud computing systems work and keeping them safe because it is basically a system where a lot of computers in a network work together to record things like transactions in a way that is clear and cannot be changed, and it does this by keeping every transaction in a block that is linked to the one before it using special codes, so it makes a strong chain that no one can easily break or change, and because it doesn’t need any big companies or middlemen to control it, blockchain fits really well with decentralized cloud systems which also don’t have a central authority. One of the

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

main things that blockchain does is making sure that data stays the same and is not messed with by keeping all the records in one place where everyone can see them, so if someone tries to change or play with the data, it will be really easy to notice, and this makes people trust the system more because they can check everything on their own without needing to rely on someone else to tell them it's correct. Another thing is that blockchain uses very smart math and codes to keep private information safe so that nobody who shouldn't see it can get to it, and it also helps make decisions in decentralized systems by using ways like Proof of Work or Proof of Stake, which are methods that let all the computers in the system agree on what is right without needing one big company to decide, and these methods help the whole system stay fair and work well for everyone. [5]

3. Blockchain for Enhancement of Decentralized Cloud Computing

Blockchain technology is changing decentralized cloud computing by fixing big problems with regular centralized systems because it gives a safe and open way to manage and store data, where in normal cloud computing big companies control everything by running servers, but this has issues like everything depending on one place, risks of data being stolen, and not being clear about what is happening, while blockchain solves this by spreading data across a lot of computers where every computer has a full copy of the data, and this way no single company or person has control over it which makes it much safer and less risky. One of the main good things about blockchain in decentralized clouds is that it keeps everything honest and clear because every transaction or change to data is recorded in a way that cannot be changed and everyone in the network can see it, so anyone can check if the data is right and see if something has been changed, and this is super important in areas like healthcare, banking, and managing goods, where it's really important to trust the information and make sure it's correct. Another smart thing blockchain does is use something called smart contracts, which are like deals that automatically happen when certain conditions are met, so people don't have to depend on others to make things work because these contracts do it themselves, and this saves time, avoids mistakes, and cuts down on costs since no middleman is needed, and in decentralized clouds smart contracts can make things smoother by handling stuff like sharing resources, making payments, or making sure services are delivered as promised. When blockchain works together with decentralized clouds, it can really change how cloud services work by solving problems related to safety, speed, and being clear, and it can help make cloud systems better for everyone, as shown in figure 2. [6]

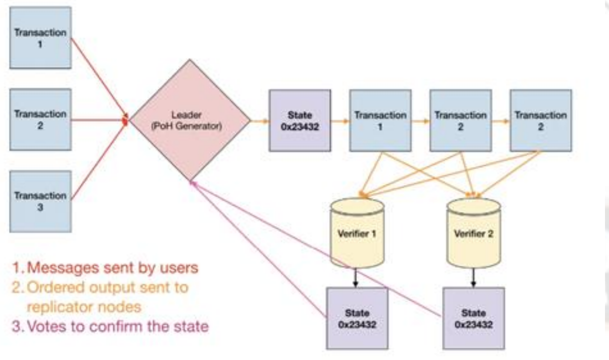

Fig. 2. Blockchain Enhances Decentralized Cloud Computing

3.1. Security Improvements

The security of decentralized cloud computing becomes much better when blockchain technology is used because normal centralized cloud systems have big risks like being attacked from inside, hacked, or having data stolen, but blockchain gives a safe and spread-out way to manage and store data, which helps to lower these dangers a lot since instead of keeping all the data in one place like centralized systems do, blockchain spreads it to many computers where each one has a full copy of the data so even if one computer gets attacked the rest can check and fix the problem, which means hackers can't break the system easily. Blockchain also uses very strong ways of protecting data with cryptography because each block of data is connected to the one before it in a way that makes it almost impossible to change without changing everything after it, and doing that would take so much time and computer power that it's not practical, so this keeps the data safe and unchanged unless everyone in the network agrees to it. Another way blockchain makes things safer is by using methods like Proof of Work or Proof of Stake, which are systems where everyone in the network agrees that a transaction is real before it gets added to the blockchain, and this stops bad people from messing with the system and keeps everything working properly. Smart contracts also make things even safer because these are like small programs that automatically do what they're supposed to when certain conditions are met, so there's no need for a middleman and less chance of mistakes or fraud, which makes sure agreements are followed and things work smoothly, and all these features together—like spreading out data, using strong cryptography, making everyone agree on changes, and having smart contracts—create a very safe and smart system for managing data that can lead to new and reliable cloud solutions. [7]

3.2 Data Integrity and Transparency

Making sure that digital information is trustworthy needs two very important things which are transparency and keeping the data correct, because when data is used it must always stay the same without any changes so people can trust it and believe it is correct, and transparency means that everyone can see how the data is being handled and also know where it

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

comes from, which helps people to trust the process and work together, and this is very important for stopping anyone from messing with the data or cheating or doing bad things to the system, so to make sure the data stays the same, some steps are used like checking for errors, making sure the data is valid, and using special codes called cryptographic hashes that make it easy to see if anything is changed, and there are also special technologies like cryptographic algorithms and checksums which help to protect the data while it is moving from one place to another or even when it is being kept somewhere, so everything works together to make sure the data is safe and people can trust it. [8]

3.3 Decentralized Storage Solutions

Decentralized storage is a big new way of keeping data that changes how data is saved shared and used because instead of putting all the data in one place like in normal storage where one company or server keeps everything, this new system spreads the data across many computers or devices that are connected in a network, and this gives many good things like making the data safer, easier to get, and harder for anyone to block or mess up, so in regular systems if the main server gets broken or hacked all the data can be lost or stolen but in decentralized systems the data is split into pieces and kept on many different nodes which means even if one node is attacked the other data stays safe, and also many of these systems use strong encryption to make sure only the right people can see or use the data, and another great thing about this system is it makes the data easier to reach because in regular systems if the main server goes down people can't get their data but here since the data is spread out in many places it can be found from other nodes, and there are tools like IPFS which is a special way for people to share and save files without needing a big central server and also systems like Filecoin where people can give their extra storage space to others and get paid with cryptocurrency for it, so this system is really changing how data is handled and making it better in many ways cryptocurrency as shown in figure 3. [9]

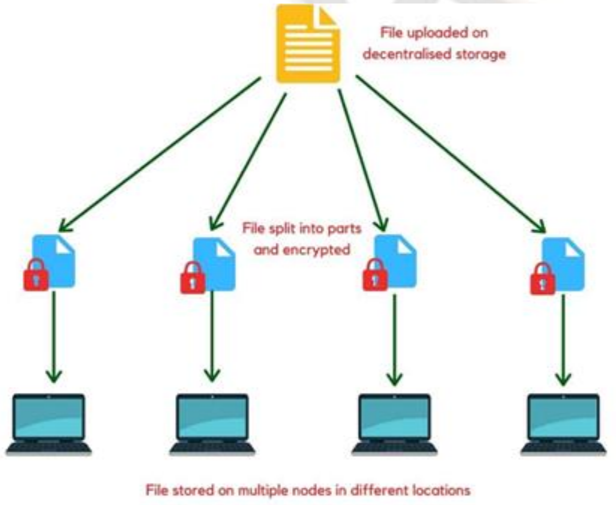
File uploaded on decentralised storage
File split into parts and encrypted
File stored on multiple nodes in different locations

Fig. 3. Decentralized Storage Solutions

Another platform called Storj provides decentralized storage which gives users an additional layer of security and privacy by storing encrypted data on a global network of nodes. In conclusion decentralized storage options offer a good alternative to traditional centralized systems. They distribute data across a network of nodes improving data availability security and resilience to censorship and breaches. A vital component of the digital infrastructure decentralized storage is anticipated to be important in data management going forward because of the growing need for reliable and secure data storage especially for sensitive applications. [10]

4. Decentralized Cloud Computing: An Overview

Decentralized cloud computing is an innovative and ground-breaking method of providing cloud services in contrast to traditional centralized cloud computing models. Decentralized cloud computing distributes data processing storage and computing responsibilities across a network of distinct nodes in contrast to traditional cloud services that rely on centralized data centers managed by a few strong corporations such as Microsoft Azure Google Cloud or Amazon Web Services (AWS). Examples of nodes that provide resources to the network include personal computers servers and even mobile devices. The decentralized model democratizes access to computer resources while enhancing security resilience and user control over data. Lets take a closer look at each facet of decentralized cloud computing. [11][12]

4.1. Definition

The centralization that is frequently seen in traditional cloud computing models is eliminated by fundamentally decentralized cloud computing. With services provided from centralized data centers traditional systems depend on a single entity to manage their resources and data. This centralization frequently results in security outages and data breaches. Decentralized cloud computing in contrast distributes computing power among a network of nodes that may be spread out over multiple different regions. Allowing various entities to independently own and operate these nodes can result in a more reliable and scalable system. Every node in the network contributes a portion of the total processing power and storage by cooperating with the others. It eliminates the single points of failure that are common in centralized systems making it a very robust system. Even if some nodes fail or are compromised the system as a whole continues to function normally with the remaining nodes taking over. Additionally by ensuring that no single entity has total control over all data the infrastructures decentralized design enhances security and gives users more control over their personal information. [13]

4.2. Decentralized Cloud Computings main benefits. Increased Security.

One of the biggest reasons why decentralized cloud computing is better is that it makes security much stronger, because in normal cloud systems, all the data and apps are stored in big data centers, and hackers and bad people like to target them, and if one of these servers gets hacked, it can affect millions of users and expose a lot of data, and the companies running these big servers are the ones responsible for keeping the data safe, so if they make a mistake, it could lead to a breach, but in decentralized cloud computing, the data and work are spread out across many different nodes, and because of this spread, even if one node gets hacked, the data on the other nodes stays safe, so it's much harder for attackers to mess up everything, and these systems also use strong encryption to protect data so that only the right people can access it and no one can change it, which makes decentralized cloud computing much safer against hackers and reduces the chance of a data breach, and also, in normal cloud systems, problems like server failures, outages in data centers, or issues with the network are the main reasons why the system goes down, and for businesses that need to always be online, these problems can be really bad because they make important apps and services stop working for a long time, but decentralized cloud computing fixes this problem by spreading the work across many different nodes, so if one fails, the system can still keep working.

4.3. Essential Ideas in Decentralized Cloud Computing.

Knowing the fundamental ideas that underpin this model is crucial to gaining a deeper understanding of decentralized cloud computing. Peer-to-peer networks blockchain technology smart contracts tokenization decentralization and interoperability are a few of these. Lets investigate these ideas. separation of powers. The core idea behind the decentralized cloud computing paradigm as a whole is decentralization. While decentralization disperses control and decision-making throughout the network traditional cloud computing concentrates all data and control in one place. This guarantees the systems overall resilience and lowers the risks related to single points of failure like server outages or cyberattacks. peer-to-peer systems. A decentralized cloud model eliminates the need for a central server by allowing nodes to communicate directly with one another. Peer-to-peer (P2P) networks facilitate the efficient sharing of resources data and computational tasks among nodes. Because every node can both consume and provide resources cooperation and resource sharing are encouraged. P2P networks which enable the safe and decentralized exchange of resources are a fundamental component of decentralized cloud computing. Blockchain technology. A distributed ledger technology called blockchain makes sure that data is safe and unchangeable by recording transactions across several computers. Blockchain is the cornerstone of decentralized cloud computing guaranteeing the integrity security and transparency of transactions. [14]

4.4. Blockchains function within decentralized cloud computing

Blockchain is not merely a technology that makes decentralized cloud computing possible it is the core technology that makes decentralized cloud systems safe and effective. In this context blockchain technology offers a number of significant advantages. security and unchangeability. Since the blockchain is decentralized data stored on it is immutable—that is once it is recorded it cannot be changed or removed. Blockchain technology is perfect for decentralized cloud computing because of its tamper-proof feature which ensures the security and integrity of data and transactions. Security is further strengthened by the decentralized consensus mechanisms of blockchain which also render it impervious to malicious activity or attacks. Decentralized Consensus. Consensus techniques like PoW and PoS are used by blockchain to verify transactions and preserve network integrity. By guaranteeing that the blockchain cannot be controlled by a single entity these mechanisms encourage decentralization and guard against fraud and manipulation. intelligent contracts. When it comes to automating the management of decentralized cloud resources smart contracts are essential. These contracts make sure that resources are distributed and billed equitably by executing automatically when certain requirements are satisfied. By lowering dependency on middlemen smart contracts increase productivity and lower the possibility of disagreements. incentives and tokenization. [15][16]

5. Public Blockchains

5.1 Public blockchains

Public blockchains are the most open and fair type of blockchain, which allows anyone from anywhere in the world to join and take part, and because these networks use a system where everyone agrees on what happens, all users can access, approve, and suggest transactions, and all the people can see the public ledger where all the transactions are saved, so public blockchains are very trustworthy and clear, and the first cryptocurrency Bitcoin is a good example of a public blockchain, and Ethereum took it even further by adding smart contracts that help make decentralized apps (dApps) easier to build, and public blockchains are really good because they're very safe, and since the control of the network is shared between many different computers, it’s almost impossible for just one person to mess with or break the system, and this way, it’s also really strong against fraud and hacking, and since public blockchains are open to everyone, anyone can check and verify the transactions, which builds trust, and because everything is so clear and open, public blockchains work really well for things that need to be honest and checkable, but there are big problems with public blockchains, especially because they're spread out so much, which makes them slow and hard to handle large amounts of data.

5.2. Private Blockchains

Private blockchains which are also called permissioned blockchains work very differently from public blockchains because they only let certain people join in and they have more control over the network so they are better for businesses and industries that need better security and privacy and also need to handle more transactions, and private blockchains are run by one main company or a group of trustworthy organizations that give people permission to use the network for things like reading, writing, or checking transactions, and this makes private blockchains really good for industries where it's super important to keep things private and work efficiently like in supply chain management, healthcare, and finance, and one of the big advantages of private blockchains is that they keep data private, so sensitive things like financial details or medical records can be shared safely within a small group of trusted people without worrying about people who shouldn't see them, and this is really important for businesses that have to follow strict rules about how they handle data and need to keep things private, and private blockchains are also faster than public ones because they have fewer users, so transactions can be done quicker and with less work for the computers, which means they are cheaper and faster to use, and another good thing about private blockchains is that they can be changed and adjusted by the businesses to fit what they need, and even though they have their own problems like having one central authority in control and not being as open, they still have a lot of good uses for companies that want to make sure their operations are safe and fast, and private blockchains are really helpful for industries that want to take advantage of the power of blockchain technology to make their work better and faster in cloud computing. [17]

6. Benefits of Using Blockchain in Decentralized Cloud Computing

Applying blockchain technology to decentralized cloud computing have many good points and it is changing how we handle and store data in better way. One of the biggest thing is more security because the old cloud computing with big servers is easy to hack and get data so that is a risk but blockchain uses many networks and special math things to keep data safe and make it harder for bad people to attack. Blockchain also have this thing called distributed ledger which keep track of every little data and transaction so no one can change anything without people seeing it, and this helps to trust more and make everything clear. Because of this, everyone can see the truth about all the data and check it for being right, and this can help make less fights and problems in things like supply chains or anything where people need to trust the process. Also, the way blockchain keeps data is safer and better because in the old cloud computing systems, if one server breaks, all the data can go away but with blockchain, the data is spread over many places so it will still be there if one goes down, making it a lot stronger and more reliable. Another thing blockchain helps with is saving money, because it doesn't need a lot of people or businesses in middle to handle the data, and that cuts costs. Users can talk directly to the system and not need many other services, plus smart contracts help by making jobs automatic so things get done faster and cheaper. To sum it up, using blockchain with decentralized cloud computing gives us more security, trust, better data, cheaper services, more control over the data, and it works with other systems easily, so it solves many problems from old cloud ways and makes a better, safer, and more reliable way of handling data. As blockchain keeps getting better, it will keep growing and changing many industries and ideas grow in popularity as it develops and matures spurring innovation and revolutionizing a number of sectors. [18]

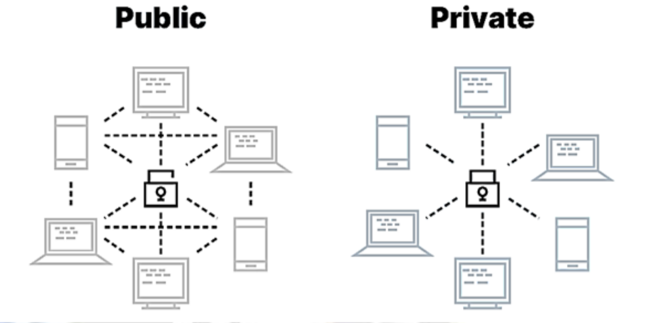

Fig. 4. Public And Private Blockchain

6.1 Enhanced Security

Enhanced security is one of the main advantages of combining blockchain technology with decentralized cloud computing. With data breaches cyberattacks and unauthorized access becoming commonplace blockchain-based solutions offer a robust defense against sensitive data. Unlike conventional cloud systems that depend on centralized servers blockchain uses a decentralized network architecture which inherently reduces vulnerabilities. Because these systems lack a single point of failure they are resistant to a wide range of attacks including Distributed Denial of Service (DDoS) and system-wide lapses. Blockchains decentralized ledger serves as the first line of defense. All data entries and transactions are cryptographically secured and appended to a sequence of blocks in order to produce an unchangeable verifiable record. This makes it impossible for data to be secretly altered after it has been recorded. Since large-scale blockchains are nearly impossible to modify any attempt to do so requires control over the majority of the networks nodes. The degree of integrity offered by this immutability which shields data from both internal and external threats is unmatched by conventional cloud storage systems. Cryptographic algorithms offer an extra degree of security. Blockchain systems safeguard data storage and transactions using advanced encryption techniques like SHA-256 and elliptic curve cryptography. Even if data is intercepted this encryption ensures that unauthorized parties cannot decode it. To prevent unwanted decryption for instance confidential company documents stored in a blockchain-powered cloud would be encrypted even if hackers were able to obtain the raw data. Additional security measures include multi-signature protocols and private key mechanisms. Obtaining information or conducting transactions in decentralized blockchain-based systems usually requires the approval of multiple parties. [19]

6.2. Cost-effectiveness

Cost effectiveness is a fundamental goal for businesses and organizations since it directly affects sustainability and profitability. To achieve cost efficiency waste must be reduced output must be increased costs must be reduced and resources must be optimized. Many strategies and processes can be used to reduce operating and technological costs. Adoption of cloud computing is one of the key tactics for achieving cost effectiveness. Businesses can access computer resources like storage processing power and software through pay-as-you-go cloud computing. Because there is no longer a need for significant upfront investments in hardware and infrastructure capital expenditures have decreased. Additionally cloud services can be scaled up or down to meet demand ensuring that companies only pay for the resources they actually use. This flexibility and scalability help to reduce overall costs and improve operational effectiveness. Automating processes is another crucial element in achieving cost effectiveness. By automating repetitive and time-consuming tasks organizations can reduce the need for manual labor minimize errors and increase productivity. Automation can help with many processes such as data entry for supply chain management and customer service. Staff members can focus on more strategic and valuable work by using robotic process automation (RPA) to handle routine administrative tasks. As a whole cost effectiveness is a difficult goal that can be achieved through a variety of strategies including energy efficiency cloud computing outsourcing and supply chain management automation. Through cost reduction and resource optimization organizations can increase overall operational performance sustainability and profitability. [20]

6.3. Improved Data Privacy

Businesses collect a lot of data from people, and it’s very important to keep this data safe from people who should not see it or use it, and this is what data privacy is all about, which means making sure nobody can take or destroy personal data without permission, and this is important to make people trust the business, follow the rules, and stop bad things like hackers stealing the data, so to do this, businesses need to have strong rules about how they get, keep, and use data, and these rules should say what kind of data can be taken, what it can be used for, and how long it can be kept for, and when businesses have these strong rules, they can make sure that the data is not used wrongly or seen by people who shouldn't see it, and one of the best ways to keep data safe is by using encryption, which is a way of turning data into unreadable code so that even if someone steals it, they cannot understand it, and when the data is moving or stored, businesses use things like AES to make it really safe, and there is also something called end-to-end encryption which means only the person who sends the data and the one who gets it can see it, and also, businesses can use ways like anonymizing data, which means taking away the personal information that could tell who the person is, and they can also use pseudonymization, which means replacing personal details with fake names so that only some other special info can connect it back to a person, and these ways help businesses keep data safe and follow the laws, and businesses also need to follow laws like CCPA in the US and GDPR in Europe, and these laws tell businesses how they should collect, use, and keep people's data safe, and businesses have to ask people if it's okay to take their data, be honest about what they do with it, and stop anyone from stealing or using it without permission, and businesses also need to make sure that the people working there know how to keep data safe by teaching them things like using strong passwords, spotting fake emails, and following the rules about how to handle data safely, and by doing training and reminding workers often, businesses can avoid mistakes that can lead to data leaks and also help make everyone in the business care about keeping data safe. [21]

6.4. Increased Reliability and Uptime

Two significant advantages of blockchain-powered decentralized cloud computing are increased dependability and uptime. Data loss and significant outages are among the issues that traditional centralized cloud services commonly encounter due to single points of failure. Reliability and uptime are significantly increased by decentralized cloud computing which divides data and processing duties among multiple network nodes. Eliminating single points of failure is a major factor in decentralized cloud computings increased reliability. If the main server or data center experiences an outage the entire service could be disrupted in a centralized system. In contrast a decentralized system has numerous nodes that distribute data and applications. In the event that a node fails the system can still operate with other nodes to guarantee continuous availability. Having this redundancy is crucial for improving dependability and uptime. Blockchain technology provides a secure immutable ledger for recording data and transactions which further increases reliability. To ensure data integrity and prevent manipulation multiple nodes validate every transaction. By reducing the likelihood of data corruption and unauthorized access this decentralized verification process improves the overall dependability of the system. Reliability and trust are further enhanced by blockchain consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) which ensure that all nodes agree on the networks current state. Reliability and uptime are two key benefits of decentralized cloud computing made possible by blockchain technology. By removing single points of failure storing data securely and irrevocably integrating edge computing and rapidly recovering from failures cloud infrastructure becomes more robust and dependable. Decentralized systems enhanced dependability and uptime can provide individuals and businesses with a competitive advantage and ensure uninterrupted service availability as they increasingly rely on cloud services for critical functions. [22]

7. Challenges in Implementing Blockchain for Decentralized Cloud Computing

Although there are many potential advantages to blockchain technology for decentralized cloud computing several problems must be fixed before these advantages can be fully realized. Among these challenges are those related to scalability interoperability regulatory and compliance and the challenge of integrating blockchain technology with existing systems.

7.1. Scalability Issues

Scalability is a significant barrier to the implementation of blockchain for decentralized cloud computing. Blockchain networks often struggle to process large numbers of transactions quickly especially those that use Proof of Work (PoW) consensus mechanisms. This limitation could reduce the effectiveness and efficiency of decentralized cloud computing platforms especially as the number of users and transactions increases. The time and processing power required to validate and add new blocks to the chain are the main causes of scalability issues with blockchain networks. Miners compete to validate transactions and create new blocks in PoW-based blockchains by solving challenging mathematical puzzles. This process is time-consuming and resource-intensive which leads to slower transaction processing times and a limited throughput. The Bitcoin network can only process approximately 15 transactions per second while the Ethereum network can process up to 15 transactions per second. Sharding is another effective solution for scalability issues. The blockchain network is split up into smaller more manageable chunks called shards through the sharding process. It is possible to handle multiple transactions at once because each shard can process transactions independently. For more on scalability see Scaling the Future: Blockchain Scalability and Quantum Computing: Blockchain Security and Scalability 2024.

7.2. Regulatory and Compliance Concerns

Regulatory and compliance concerns are important when using and implementing user proxies especially in industries that handle sensitive data such as banking healthcare and telecommunications. Regulatory frameworks such as the General Data Protection Regulation (GDPR) in Europe the Health Insurance Portability and Accountability Act (HIPAA) in the US and many other national and international laws enforce strict guidelines for data security and privacy. For businesses ensuring that the use of proxies does not violate these regulations can be challenging and complex. Among the most important concerns is data privacy. Proxy servers are commonly used to handle vast volumes of user data including sensitive and private information. Ensuring that this data is anonymized and protected from unauthorized access is crucial. Violating data protection laws can have major repercussions including hefty fines and reputational damage. In conclusion businesses that employ user proxies need to consider compliance and regulatory concerns. Meeting the requirements for data privacy data sovereignty and transparency is essential to avoiding legal issues and maintaining public trust. In order to mitigate these risks organizations must implement robust compliance frameworks and stay abreast of evolving regulatory landscapes.

7.3. Technical Complexity

The technical intricacy of user proxies is another significant problem that organizations handle. Using and maintaining proxies requires a deep comprehension of data management strategies and network architecture security protocols. This complexity may make it challenging for businesses without the necessary technical know-how and resources to enter the market. One of the biggest technical challenges is ensuring that proxies work seamlessly with the existing IT setup. To manage various traffic types including HTTP HTTPS and FTP without interfering with normal business operations proxies must be set up. This necessitates careful planning and coordination with network administrators and IT teams. In addition proxies must be scalable to ensure high availability and performance while handling varying traffic volumes. Security is another essential element that contributes significantly to the technical complexity of proxies. In order to protect against a variety of online threats including Distributed Denial of Service (DDoS) attacks and malware data breaches proxies must be configured. This requires the implementation of robust security measures such as intrusion detection systems firewalls and encryption. Regular security updates and assessments are also necessary to handle emerging threats and vulnerabilities. Monitoring and analyzing network traffic is another aspect of proxy management that is necessary to identify and address performance issues. Sophisticated monitoring techniques and tools are required for real-time data collection and analysis. [23]

7.4. Energy Consumption

Using proxies for users uses a lot of energy and because people are more worried about how much energy we use and how it affects the environment, this is something that needs to be thought about because just like other things in a

***Article Received:** 25 July 2022 **Revised:** 12 September 2022 **Accepted:** 30 November 2022*

network, proxies need energy to work and send and get data, and the more energy they use, the more problems it can cause both with money and with the environment, and the reason proxies use so much energy is because they run on servers that always need power, and these servers are usually in places like data centers that have special systems to keep them from getting too hot and these systems take even more energy to keep the servers running, and the servers use a lot of power especially when proxies are being used by a lot of people or for big tasks, and it's not just the energy the servers use that is a problem but also the extra energy that comes from the traffic on the network because proxies send and store requests which can make the traffic grow and this causes the network to use more energy, and this is especially true in places like big company networks or when delivering content where proxies have to deal with a lot of data coming through, and businesses also have to think about how to make the systems they use for proxies work better so they don't waste energy, and they can do this by picking hardware that uses less energy and by setting up proxies in a way that helps them use less power, and they can also make sure the traffic is shared out well between different servers so they don't need as many servers and don't waste energy, and another good idea is to try using energy from things like wind or solar to power the servers because more data centers are using these renewable energy sources now to try and cut down on pollution and help save the environment.

8. Future of Blockchain in Decentralized Cloud Computing

The future of data access management and storage could be drastically changed by blockchain technology in decentralized cloud computing. Blockchain technology is a good alternative to traditional cloud computing models which have problems with security privacy and centralization. By using blockchains decentralized architecture cloud computing can become more transparent secure and resilient. This change could impact a wide range of industries including supply chain management healthcare and finance.

8.1. Emerging Trends

One of the most significant new developments in blockchains future for decentralized cloud computing is the rise of decentralized storage solutions. Traditional cloud storage providers like Google Cloud and Amazon Web Services (AWS) rely on centralized data centers which are vulnerable to cyberattacks and data breaches. Blockchain technology is used by decentralized storage platforms such as Filecoin and Storj to distribute data across a network of nodes preventing a single point of failure. This approach increases data security and privacy because users can encrypt their data before storing it on the network and still have control over it. Another recent development is the fusion of blockchain technology and edge computing. Edge computing reduces latency and increases efficiency by processing data closer to the source. Decentralized cloud networks can achieve greater scalability and efficiency by combining edge computing and blockchain technology. For example initiatives like IoTeX are looking into using blockchain technology to secure data generated by Internet of Things (IoT) devices at the edge of networks.

8.2. Potential Innovations

Blockchain can change a lot of things in how we use cloud computing in the future, and one big area where it could help is with creating ways for people to have control over their own online identities without needing to depend on big companies or central places that can get hacked and cause problems, so with blockchain, projects like uPort and Sovrin are trying to give users power over their own identities online so they can keep their information safe and access cloud services without worrying about centralized systems, and another thing blockchain could do is help create new ways to buy and sell computing resources because right now in normal cloud computing, people usually just buy from one provider but with blockchain, people can make a marketplace where they can directly trade resources like processing power with each other without needing to rely on one company, and projects like Golem and iExec are already trying this idea where people can rent out their extra computing power to others and save money while using things more efficiently, and smart contracts, which are like automatic agreements that just happen when certain rules are met, could also play a big role in how blockchain works in decentralized cloud computing because they help make things faster by doing processes like paying, sharing data, or giving out resources automatically without needing someone in the middle to manage it all, and this could really change the way cloud computing works and make it cheaper and safer. [24][25]

9. Conclusion

In the end its so so important for companies to have solutions that fit their needs and also use proven methods to do well in business today where things are always changing and getting harder because when companies make sure their strategies and tools match what they need they can stay ahead of others and reach their goals easier and also save money, make work faster, have better security, and use their resources smarter by focusing on what makes them different and not just using the same old things everyone uses but also by making sure they use well known methods like Balanced Scorecard or Agile and things like that cause these methods have been used and proven to work well and help companies do their job better by managing projects, improving processes, and making sure things are done right every time so by mixing both custom solutions and these proven methods businesses can deal with today's tough environment better and be more successful by improving their customers' happiness, running things smoother and getting long-term success, so the future will depend on how good companies are at changing, being creative, and finding new ways to stay ahead. It’s also really helpful to summarize the key points in talks or papers cause it helps people understand and remember the important stuff better especially when there’s a lot of info to share like in business meetings, schools or when explaining complicated ideas, so when teachers or leaders repeat the main things in a talk or meeting it helps everyone get clear on what was said, what needs to be done next and also helps people in class or work not forget the key ideas they need to focus on later, like when a project manager reminds everyone about what happened in a meeting and what the next steps are so no one forgets and everything stays on track, and also in writing like reports and articles, the conclusion helps make sure the reader remembers the main findings and gets the big picture of what was discussed, and in public speaking remembering and saying the key points again helps the audience really get the message and take it home. Looking ahead, blockchain has a lot of potential to change how cloud computing works, making things more secure, cheaper, and transparent and its especially important as the world gets more digital and people need better ways to manage their data safely, and the cool thing about blockchain in cloud computing is it makes things more secure than normal cloud systems that can get hacked because everything in blockchain is spread out on different nodes and not controlled by one company so it’s harder for things to go wrong or get stolen, plus blockchain keeps track of everything in a public ledger that anyone can see so it’s easier to trust that data won’t be messed with, and using smart contracts can help businesses automatically follow agreements without needing a middle person which can save even more money and time, and in the end using blockchain for decentralized cloud computing is a smart way to get rid of the issues with old cloud systems and it’s a way to make data management cheaper, safer, and more efficient and even though there are challenges with technology and rules right now, blockchain is growing fast and will be a big part of the future of cloud computing.

REFERENCES

[1]. Wu, X., Kumar, V., Quinlan, J. R., Ghosh, J., Yang, Q., Motoda, H., ... & Zaniolo, C. (2007). Top 10 algorithms in data mining. Knowledge and Information Systems, 14(1), 1-37.

[2]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[3]. Kshetri, N. (2017). Blockchain’s roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027-1038.

[4]. Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[5]. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In Advances in Computers (Vol. 111, pp. 1-41). Elsevier.

[6]. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10.

[7]. Wang, H., He, D., Wang, Q., Huang, X., Choo, K. K. R., & Kumar, N. (2019). Blockchain-based secure data sharing for autonomous connected vehicles in smart cities. IEEE Transactions on Vehicular Technology, 68(9), 8780-8790.

[8]. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 1-8.

[9]. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37.

[10]. Nguyen, Q. K. (2016). Blockchain - A financial technology for future sustainable development. In 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD) (pp. 51-54). IEEE.

[11]. Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653-659.

[12]. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6-19.

[13]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

[14]. Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. In Architecture for Blockchain Applications (pp. 1-29). Springer.

[15]. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based machine learning for edge-of-things devices. IEEE Internet of Things Journal, 6(3), 5425-5432.

[16]. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7, 22328-22370.

[17]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd

International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[18]. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Transactions on Industrial Informatics, 13(6), 3154-3164.

[19]. Wüst, K., & Gervais, A. (2017). Do you need a blockchain? In 2017 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45-54). IEEE.

[20]. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. In 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA) (pp. 182-191). IEEE.

[21]. Mahajan, Lavish, et al. "DESIGN OF WIRELESS DATA ACQUISITION AND CONTROL SYSTEM USING LEGO TECHNIQUE." International Journal of Advance Research in Engineering, Science & Technology 2.5 (2015): 352-356.

[22]. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

[23]. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.

[24]. Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527-535.

[25]. Fu, S., Xue, Y., Xu, X., Zhang, X., Xu, J., & Zhang, X. (2018). Adaptive distributed authentication with blockchain for 5G-enabled IoT. IEEE Transactions on Industrial Informatics, 14(6), 2704-2712.