UDC: 004.76:004.63.056.55
Review article

ENHANCING SECURITY IN DISTRIBUTED CLOUD STORAGE USING BLOCKCHAIN AND SMART CONTRACTS

Nadije JAKUPI[1*], Puhiza ISENI[1*], Suela RUSHITI[1*], Jetmir QAZIMI[1*]

[1]Department of Informatics, Faculty of Natural Sciences and Mathematics, University of Tetova, North Macedonia
*Corresponding author e-mail: n.jakupi318008@unite.edu.mk, puhiza.iseni@unite.edu.mk, s.rushiti222501@unite.edu.mk, j.qazimi222400@unite.edu.mk

Abstract

Since more users are moving to cloud computing, keeping our data safe and private now matters more. Since most cloud storage is run from just one location, it is easier for attackers and causes issues if the system fails. We come up with a new way to secure cloud storage by using blockchain technology and smart contracts. Blockchain mainly allows us to have a safe and distributed record that ensures data access can be trusted. By using smart contracts, we enable people to safely access data without any help from a middleman. It means that you can see every use of data access in the system, and these actions cannot be deleted or changed.
Using blockchain technology with distributed storage, we ensure that everything happening is recorded and access is regulated correctly. We also discuss a case study to illustrate how our idea helps with transparency and trust, while at the same time mentioning concerns such as how far it can be used and problems with regulations, and our solutions for these issues.

Keywords: security, cloud, smart contracts, blockchain, cloud storage.

1. Introduction

Blockchain is now one of the central topics in computer science and financial technology (FinTech). A survey carried out by Juniper Research and published in July 2017 revealed that over half of the globe's leading corporations are examining the use of blockchain. Blockchain is a digital file of information that is secure, shareable, transparent, and unchangeable. Thanks to transparency, the data on the internet can be located and verified.
Because information technology keeps advancing rapidly and cloud services are used more widely, keeping data secure has become very important. When data is stored on a centralized cloud system, it is at risk from failures and attacks by people without permission. It is vital to introduce new security practices that guarantee reliability, openness, and protection from fraud when organizations begin using distributed architecture systems. This research looks into how blockchain technology, in combination with smart contracts, could help fix security problems.

2. Issues in Traditional Cloud Storage

Cloud storage refers to keeping your documents in the cloud, unlike having them on a hard drive. It offers you elements of the Photos app backup and lets you control and view your photos, videos, docs, and even your backups from anywhere using the internet. Even some of the largest companies in cloud storage, such as Amazon Web Services, Dropbox, OneDrive by Microsoft, and Google Drive, place all their client data in well-guarded data centers.
People find that cloud storage offers a lot ofbenefits. Having internet makes it possible to check your data from almost anywhere in the world. This kind of luxury is very helpful for daily life.

https://doi.org/10.62792/ut.jnsm.v10.i19-20.p3090

Three, you can adjust your home’s space by either making it bigger or smaller based on your preferences. If a server from a cloud computing provider fails, your data will still be in the cloud since the copies are kept elsewhere as well. The data is automatically saved, and in case something is lost, it can easily be recovered.

Yet, centralized cloud storage offers lots of benefits, but it also poses some risks. One person handles all your information, which may make you concerned about your security and privacy. In the upcoming sections, I will discuss those possible weaknesses in more detail.

3. Technologies Used

3.1 Blockchain: Blockchain is a decentralized digital ledger that safely and transparently keeps data safe from hackers. Each individual who has a copy of this ledger uses what is called a node, which is a computer in a network.

A secure chain is created by putting data into blocks, which in turn are linked to each other via their hash. Any attempt to change the content of a block will cause that hash to change, which in turn breaks the chain and is a proof of data integrity. Also, this structure is easy to identify when tampering has occurred.

Due to the time stamping and transparency features of blockchain, any user in the network can verify and trace transactions. Also, we see in the implementation of consensus algorithms like Proof of Work and Proof of Stake, which play a role in the creation of new blocks, that transactions are verified by the network and made to be free of fraud. This technology, which we use for secure and effective data transfer and storage, is on a large scale in digital identity, supply chains, and cryptocurrency.

3.2 Smart Contracts: are a code that runs on the blockchain and has it’s ability to execute on its own once some defined conditions are met. That's the middleman out! Security and transparency and which is also what we mean by irreversibility, is what this auto-run feature brings. Also, smart contracts, by way of their reduced cost and increased trust, are put into practice in the betterment of industry processes, which include supply chain, insurance, or finance.

4. Proposed Architecture

The storage and blockchain layers to take care of our data management in the right and secure way. Since it protects data by holding it on many different servers, distributed storage is similar to local storage but better.

Also, we put on the blockchain all records and info related to each transaction and data exchange. What we do here is we make that which is recorded on the blockchain tamper-proof. With this, we can present our data via smart contracts. What we do is we set out rules which determine who has access to the system and what they are allowed to do with the data. The blockchain we use logs in a secure and easy-to-follow way all events, which include access, data changes, and other movements.

We have found integration of these elements to greatly improve the security and dependability of data, which in turn prevents illegal access to the account. As we store data in many places, we reduce the chance of a large-scale cyberattack and data loss. Supply chain management, healthcare, and finance are some of the use cases that demand strict data governance, traceability, and transparency, and benefit significantly from such an architecture.

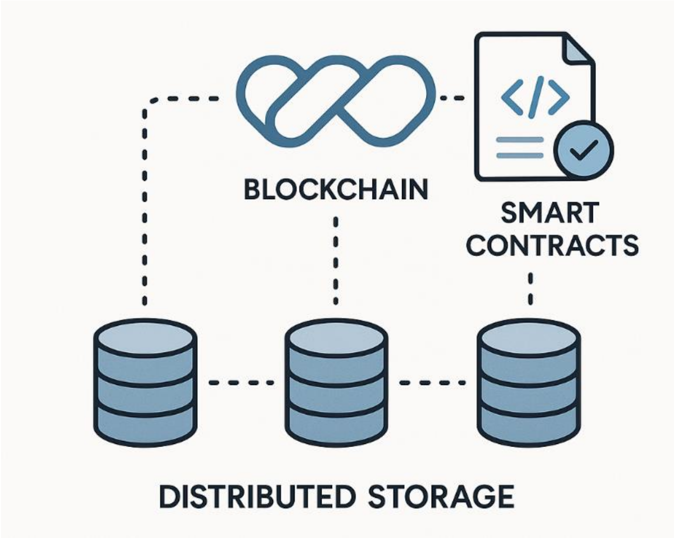

Figure 1. Proposed Architecture for Secure Data Management using Distributed Storage and Blockchain

5. Real-World Use Case

To cover all possible risks, the company is choosing to keep its confidential data in a distributed cloud storage system. The whole idea of isolating data and increasing its tolerance to errors is that files are encoded and spread across numerous nodes, avoiding being housed on a single computer.

With the help of smart contracts on the blockchain, only authorized individuals can access private documents. With the help of smart contracts, only allowed users can read, edit, or share the papers as decided by the access policies. The operation of granting or denying access is carried out by the automatic inspection of the user's credentials and permissions by the smart contract.

Every attempt to get involved, each document update, and every transaction is permanently saved in the blockchain ledger. As a result, the company can view its data use live and have a permanent record to review in case of trouble.

Also, getting rid of system administrators or outside gateways with smart contracts reduces costs and risks from people who have access to the system. If maintaining security, respecting privacy and being compliant is the foremost priority, using distributed storage together with blockchain-based access control can be very beneficial for safe access to private data.

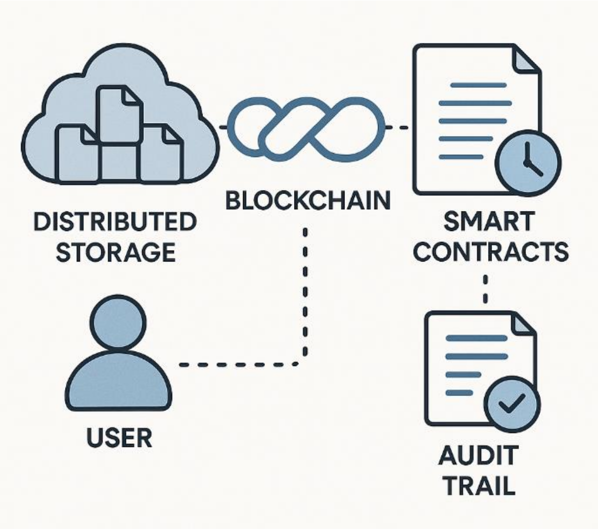

Figure 2. Real-World Implementation of Secure Data Access Using Distributed Storage and Blockchain

6. Benefits of the Approach

All operations on the data, such as accessing and changing it, are recorded and visible for everyone on the blockchain. With the blockchain's transparent history, all stakeholders will be more dependable and responsible.

Because all blocks use cryptography and belong to multiple computers, it is not easy to change information without being discovered. As a result, this makes the data remain whole and accurate over a longer period.

Smart contracts protect the system by not leaving data operations to human mistakes and by only allowing access as the rules are set. So, security enforcement is done in a standard and dependable manner.

The system prevents problems with bottlenecks and limits threats from inside by avoiding the use of central authorities or third-party intermediates. Moving processes to the users and nodes reinforces the system and gives more freedom to users.

7. Challenges and Limitations

Although it has a myriad of benefits, the proposed architecture is not without several limitations and disadvantages to be appropriately considered. Scalability of blockchain is a significant issue; the more data and transactions, the greater the chances that the network will experience slower processing times and increased fees, and this affects system performance as a whole.

Since blockchain technology is open in nature, all the players have access to transaction details, thus generating issues of privacy too. Even though information may be off-chain or encrypted, it remains challenging to maintain confidentiality in sensitive applications.

The prohibitive nature of storing huge amounts directly on-chain is another constraint. The majority of systems are founded on off-chain distributed storage paradigms owing to the reality that blockchain storage is inefficient and costly for big files, thus making it increasingly difficult to keep the data in synchronization and integrity.

Last but not least, variations in data protection laws, jurisdictional borders, and compliance requirements present worldwide legal and regulatory issues. These may make it more difficult to implement a distributed storage system based on blockchain technology across several nations or areas.

For blockchain-integrated distributed storage solutions to reach their full potential, these issues must be resolved.

8. Recommendations for the Future

Future research and development should focus on a few crucial areas in order to overcome the present obstacles and completely realize the potential of distributed storage systems coupled with blockchain technology.

First, as a means of lowering expenses and promoting the protection of data and ease of access, more effective off-chain storage models that are directly compatible with blockchain technology will have to be developed.

Secondly, it will be necessary to make sure that modifications to data protection laws—e.g., the CCPA, GDPR, and other territorial laws—are adhered to. Solutions in the future will require having access controls with flexibility that are able to accommodate different legal frameworks within jurisdictions, as well as privacy-preserving mechanisms.

Third, widespread adoption is facilitated by providing the market with systems that are open and integrate well with other solutions. We will introduce blockchain-based storage and interconnecting technology for us to make protocol rules and support novel industrial ideas additionally.

Future developments can produce more scalable, secure, and legally acceptable systems that help a variety of applications and sectors by tackling these issues.

9. Conclusion

The joining of blockchain technology, smart contracts, and distributed storage systems has greatly helped in the effort to protect data that is both open, secure, and decentralized. This method maintains the quality of data, people can trust it, and both trust and accountability are maintained without centralized groups, thanks to combining decentralized access controls with unchangeable records. Until questions about privacy, scaling, and following rules are resolved, blockchain can drive major progress in the industry. More research and development will be required to let these technologies spark real change across industries.

References

[1]. Dai, J., & Vasarhelyi, M. A. (2017). “Toward Blockchain-Based Accounting and Assurance”. Journal of Information Systems, 31(3), 5-21

[2]. Silvana Qose & Gentian Hoxhalli, “Aplikimi i teknologjisë Blockchain në sigurinë”

[3]. Rodrigo Craveiro Rodrigues, Pedro Miguel Calhau Mateus & Valderi Reis Quietinho Leithardt, “Prichain II: CloudGuardian's Proposal for Cloud Security with Blockchain”, 2024

[4]. S. M. Udhaya Sankar, D. Selvaraj, G.K. Monica dhe Jeevaa Katiravan, “A secure third-party auditing scheme based on Blockchain technology in cloud storage”, 2023

[5]. https://www.ibm.com/think/topics/blockchain

[6]. https://www.investopedia.com/terms/b/bitcoin.asp

[7]. https://knowledgecenter.ubt-uni.net/cgi/viewcontent.cgi?article=2285&amp;context=etd