Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7632467

SMART CONTRACT ON BLOCKCHAIN FOR IOT SCALABLE DATA SHARING: SMART AGRICULTURE AS A CASE STUDY

RashiTanwar[1] , Dr. Kamal Malik[2] , Dr. Yogesh Chhabra[3]
[1] Computer Science Department, CT University Ludhiana, India
[2]Computer Sciences Department, CT University Ludhiana, India
[3]Computer Sciences Department, CT University Ludhiana, India
tanwar5390@gmail, kamal17203@ctuniversity.in,dryogeshchhabra@ctuniversity.in

Abstract

Due to its scattered nature, the growing Internet of Things (IoT)-based Smart Agriculture is encountering significant issues with data exchange, storage, and monitoring.IoT on a very large scale We conducted a survey of the literature and discovered that the main obstacles to using blockchain for smart agriculture are its performance, scalability, cost, and throughput. This research suggests a scalable and distributed data sharing system with integrated access control for smart agriculture to address these issues. We use a smart agricultural scenario, which has four tiers: smart agriculture, smart contracts, the Interplanetary File System (IPFS), and agriculture stakeholders, to demonstrate our methodology (to remote users).The various elements of the architecture we suggest are thoroughly explained in this document. To protect consumers' privacy, our method employs anonymous identities. Because many resource owners can use their data sharing smart contracts to add, change, or remove data sharing regulations, our strategy is completely scalable.In contrast, whenever the smart contract gets a lot of requests for policy review, our method doesn't need transaction fees. We simply release and analyse one data-sharing smart contract in order to keep things straightforward. Every copyright holder must therefore instal several smart contracts in order to safely communicate farm information among investors. We examine the operation of our proposed system on the EOS blockchain in order to demonstrate that its minimal resource requirements are outweighed by the advantages it offers in terms of security, scalability, and cost.

Keywords: Access Control, Smart Contracts, Data Sharing, Smart Agriculture, Smart Farming, Scalability, Trust

Introduction

The Internet of Things (IoT) is a group of smart, Internet-connected gadgets that can function either as a single entity or as a swarm of disparate, heterogeneous entities. Industrial control, smart environments, smart agriculture, home automation, smart cities, and smart healthcare are just a few of the areas where IoT is used. Agriculture is one of the industries that has been significantly impacted by IoT development.All humans depend on agriculture as their primary food supply, and it is also vital to the nation's economic development. Because they employ old methods, farmers produce little and make poor decisions. In order to enhance productivity, agriculture needs contemporary technologies like blockchain. We can considerably enhance

monitoring, data sharing, data storage, decision-making, and fertiliser efficiency by integrating smart agriculture with low-cost blockchain technology. According to estimates made by the Food and Agriculture Organization of the United Nations (FAO), there will be 8 billion people on the planet, including farmers, by 2025 and roughly 9.6 billion by 2050 [1].Traditional methods cannot meet the demands of the growing human population, which necessitates the deployment of scalable blockchain-based solutions. Agriculture-related sensors and other equipment must be integrated with communication and information technology in order to practise smart farming (SF).According to their demands and needs, various stakeholders produce and manage data. The implementation of smart agriculture further improves operations through the use of IoT and contemporary data collection and analysis methods. To facilitate the sharing of delicate agriculture data while maintaining privacy, existing infrastructure must handle important issues, including data sharing [2]. Traditional methods take advantage of a central server, which is prone to security flaws and single points of failure. The biggest issue with Nakamoto-consensus blockchain platforms is scalability. Although the value of the network increases with user density, smart agriculture's scalability issue remains unresolved [3]. Additionally, because of their greater costs, longer block creation times, increased transaction latency, and high processing overhead, existing blockchain technologies are not appropriate for the IoT.User transactions are organised into blocks by the "blockchain" distributed ledger system. There are a number of transactions in each block. The peer-to-peer (P2P) blockchain network broadcasts these blocks and uses network nodes to verify them. A cryptographic hash of the block that came before is included in each newly approved block when it is appended to the one that came before it. Hashing is a key part of making the blockchain more secure because if you change one block, it will change the hashes for all the blocks that come after it. As a result, competing shared ledger copies will appear, and the blockchain state willchange its consistency. Since each peer in the blockchain network has direct access to a copy of the distributed ledger, the term "shared ledger" is frequently used to refer to the blockchain. It's important to note that blockchain relies on synchronisation, in which each node interacts with other nodes to exchange requests for and imports of the most recent blockchain data. Blockchain technology has potential uses outside of Bitcoin. As opposed to conventional, centralised methods, our method offers the following benefits for smart agriculture:

• Trust: The basic characteristic of blockchain technology is the way it redefines the word "trust." The present methods for transmitting agricultural data are built on centralised systems, which are prone to individual failure points and security issues [3].Our strategy, which is built on virtual identity, safeguards user security. Additionally, to allow resource owners additional anonymity, the EOS blockchain supports financial transactions [4].
• The blockchain contains rules for data exchange without requiring changes to IoT devices, making our technique lightweight.
• Scalability: By enabling numerous resource owners to use their smart contracts to set rules for data transmission, our technique tackles the issue of scalability [5].

• High Throughput: Compared to public blockchain platforms, our method suggests using permissioned blockchains to achieve high throughput.Blockchain creates the perfect atmosphere to lessen fraud, manipulation, corruption, and the costs associated with paper-based methods in information-intensive farming. It promotes open dialogue between the government and farmers [3].

• Accessibility: With the mechanisms now in place for sharing data, a server outage could make it impossible to access the data sharing policies.However, the data sharing policies are always available thanks to our blockchain-based system.To carry out a specified task, a smart contract consists of programme code and a storage file. When users send transactions to a smart contract, the contract may read or write data to its storage file.The user creates the programmes, compiles them, and then instals them on a platform for smart contracts. Over the past few years, additional blockchain platforms that support the capabilities of smart contracts have appeared in addition to Ethereum. For example, Stellar, Monax, and EOS are developing platforms that let users create smart contracts to carry out various functions like data sharing and storage. The software code is written in a separate programming language for each platform. Typically, a contract creation transaction is used to create a new contract on the blockchain, and transactions are sent to it to execute the contract logic. The nodes that are taking part also take part in these transactions. They agree on the outcome and update the blockchain as needed.By employing anonymous public keys, blockchain users can be easily visible when they send transactions to the blockchain in order to send money or carry out instructions from smart contracts (PKs). These transactions are pushed into a block by miners, a specialised group of blockchain nodes. The block is uploaded to the blockchain after the extraction process is finished. In our earlier work [7], we suggested that leveraging blockchain for information exchange is difficult due to substantial constraints like the low application performance of present platforms, high transaction fees, and high resource utilisation to resolve the PoW consensus process. To solve these important problems, we propose a new way to share data based on the EOS blockchain. Our suggested solution is good for smart farming because it is built on a platform that is scalable, reliable, and cheap.We chose a smart farm as the setting for our ideas to be demonstrated, but our method works just as well in other IoT settings. As shown in Fig. 1, the structure of our system is divided into four tiers: smart agriculture, smart contracts, the Interplanetary File System (IPFS), and agriculture stakeholders (remote users). Current platforms' scalability and performance issues are resolved with the EOS blockchain [8]. This platform also supports decentralised applications (DAPPs), supports standard programming languages (like C++) for writing smart contracts, has cheap fees, and has the shortest block generation times. For the creation of decentralised apps and smart contracts, EOS has developed a more reliable architecture [5]. It scales to 100,000 transactions per second using the delegated proof-of-stake (DPoS) consensus process. It employs a set of public and private keys to distinguish between networked devices that have been registered. It carries out a smart contract's instructions by using accounts and transactions. For instance, to check the status of rights on the blockchain, a storage device is linked to an EOS account. Similar to this, each owner of a resource has an EOS account that they can use to add, edit, and remove permissions on the blockchain.This study's goal is to offer a comprehensive analysis of the distinctive components of our blockchain-based information solution for smart farming. We

start by outlining how transactions are processed and data is saved on the storage device. The smart contract for sharing data is hosted on a high-performance permissioned blockchain. This makes it easy to add, change, or remove rules for sharing information from the blockchain. Additionally, a blockchain creates an unchangeable history of all transactions involving access requests that can be traced back to the people who filed them. It is possible to identify security problems by analysing this log. We examine how our suggested approach mitigates security vulnerabilities like DoS assaults and qualitatively demonstrate that it achieves availability, integrity, and secrecy. Finally, we assess how well the data sharing smart contract on the EOS blockchain is performing and demonstrate that the resource usage our system causes is minimal. The remainder of this essay is structured as follows: The history and associated work are covered in Section II. The access control and data exchange framework for smart agriculture are covered in Section III. The performance assessment is presented in Section IV.Section V is the last section of this essay.

II. Beginnings and connected work

Numerous programmes have been created recently to help with the distant management and surveillance of smart farming. Applications for cellphones that measure weather conditions are receiving more attention. Such agricultural monitoring programmes are designed to provide resource owners with baseline data for future planning and alerts. Farmers, decision-makers, and consumers must all receive agricultural data while ensuring the integrity of the data is maintained. Agriculture should not use legacy IT data management systems because of security flaws, single points of failure, and data tampering. But given its intrinsic benefits, blockchain technology is a strong contender to influence the evolution of smart agriculture. Blockchain characteristics like immutability, no single point of failure, and data openness have the potential to create secure and reliable data exchange. To assure confidence and better decision-making, blockchains can gather data on agriculture from a variety of sources, including sensors, satellites,drones, and other agricultural tool [9].

In fact, blockchain technology-enabled smart agriculture is the logical next stage in the evolution of current farming practices. It is important to note that administrators now manage and store agricultural data on centralised systems. Stakeholders have faith in the administrators to maintain the security and integrity of the data. However, administrators pose a risk since they have personal agendas and interests that could jeopardise data security. For smart agriculture, new blockchain-based solutions will surface.

A pilot research study was carried out by Ge et al. [10] to determine the applicability of blockchain technology in the agrifood industry. They contend that the numerous information management issues present in current agri-food transactions make this technology very necessary. Blockchain's immutable transactions and distributed access mechanism for achieving trusted data sharing have the ability to lessen the likelihood of fraud. The study looked at a number of issues that the agriculture industry must address with blockchain technology. Some of these concerns include safeguarding data sharing, interacting with current network technology, speed, efficiency, throughput, and the price of network development. The trustworthiness of data put on the blockchain, how to select the best blockchain platform, the

consistency of smart contracts, and how well the blockchain works to prevent fraud were among the top concerns expressed by stakeholders in the agriculture industry. They identified problems with the current central data storage systems, including their increased prices, lack of integrity, and fraud because of the chances of data modification. But blockchain technology provides a tamper-proof platform to ensure the veracity of record storage and data transmission guidelines. The agricultural sector is now more trustworthy and transparent as a result of the present paradigm shift [3]. The authors, however, have only provided a theoretical framework describing the challenges that blockchain technology poses for the agriculture sector. IoT applications benefit from blockchain-based systems, according to Ferrag et al. [11]. It's critical to understand the properties of the blockchain before choosing a blockchain-based solution for an Internet of things application. They argue that several blockchain concerns, there are costs and scalability as the number of nodes in the agriculture sector grows, should have been considered. So, for IoT-based agriculture, a blockchain scalability analysis is essential. Additionally, they contend that it is crucial to protect IoT device data with privacy-preserving methods.

One of the essential security elements in smart agriculture is anonymity. In IoT applications, blockchain-based solutions enable user anonymity. The final point made in this study is the importance of finding an appropriate consensus algorithm to handle the high computational and energy demands.

Recently, Hang et al. [9] proposed a fish farming platform utilising blockchain for the integrity of agricultural data. The fish farms are remotely monitored using IoT devices. IoT sensors can collect data that can be used for study and decision-making. They contend that while blockchain technology has many benefits for lowering costs and increasing efficiency, there are some issues that still require special attention. For instance, the existing platforms' consensus methods require a lot of computer power, which increases the time it takes for transactions to be confirmed. Instead of developing a new system, blockchain has to be integrated with the current legacy system to cut costs. In order to handle the massive amount of agricultural data gathered from sensors, new data storage technologies are required. Additionally, they contend that in order to address the performance issue, a customised blockchain implementation is required.

They propose aPKI-based approach utilising the Hyperledger Fabric Platform [12] to undertaken the accuracy of farm data. They also talk about the constraints of their research, such as the risks to validity and higher implementation and assessment expenses brought on by PKI.

Farmers and stakeholders participated in a semi-structured interview performed by Jakku et al. [13] to get their thoughts on the use of data in smart farming. The analysis's findings indicate that trust and openness were major concerns for many participants. Among them are issues with the lack of confidence in laws governing data ownership. Farmers should be able to manage their data independently and restrict access to it to a select group of stakeholders. Therefore, the primary barriers to farmers using conventional smart agricultural technologies are trust and transparency. To achieve trust and sustainable development in agriculture, blockchains can help with the transparent and distributed storage and administration of agriculture data.

A blockchain-based architecture for smart agriculture has been created by Devi et al. Different sensors, such as temperature, humidity, and smoke fire control nodes, provide data to blockchain nodes. Every node in the network performs mining operations and keeps a local copy of the blockchain. The authors use smoke fire control nodes to describe their strategy. These nodes carry out a variety of operations, such as store operations to preserve fire data, access operations to obtain fire specifics, and monitor operations to track the progress of fires. On sensors spread throughout the agricultural field in various locations, the fire level information is updated continuously. To increase data transparency, this information is stored on a blockchain. The suggested method, however, makes use of the Ethereumblockchain for data storage. The writers are motivated to find solutions to the issues with scalability, affordability, and performance.

According to Chen et al. [2], the foundation for monitoring agriculture and forestry is data related to these industries. They provide a mechanism for exchanging sensor data from forestry and agriculture. Five components make up their centrally managed data sharing platform: the data centre subsystem, the data adapter subsystem, the data storage subsystem, the data publishing subsystem, and the data transmission system. The sensor node's basic information is registered by the data centre subsystem. Data from numerous sensors is collected and analysed by the data adapter subsystem. Data storage is handled by the storage subsystem, and data query interfaces are provided by the publishing subsystem. The transmission system also handles the sensor data delivery. This server-type system is built on pricey components that are inappropriate for resource owners.

The potential applications of smart contracts in Internet of Things-based smart agriculture are shown in a recent exploratory research by Voutos et al. [15]. They claim that smart contracts can help supply chains for agriculture, logistics, and inventory. Data delievers by theIoT-based smart agriculture system and the parties' agreement are used to build the dynamic circumstances of smart contracts.

Crop quality, growth, and production are influenced by variables including the climate and the soil. IoT sensors must therefore enable logging capability and ensure dependable data transport. IoT technology can be very useful for smart agriculture.

First, intelligent sensors are useful in determining which areas are appropriate for agriculture. Second, IoT technology is crucial for determining how well a crop is doing after a tragic event. This study also shows how much data there is about agriculture and how it needs to be stored in a way that is distributed and scalable. The authors explain how to create contracts using Python, C++, and Solidity, three smart contract programming languages[20-23].To meet stakeholder expectations, the study on blockchain integration with smart agriculture is still in its early stages and faces a number of hurdles. To the best of our knowledge, this research is the first to address these important data sharing difficulties. Our research gives the agriculture sector the essential groundwork to address other issues.

III. A Blockchain-Based Data Sharing System

Fig. 1 depicts the layout of our recommended blockchain-based access management and data sharing system for smart agriculture. The IPFS storage device, numerous servers, an IoT

gateway, smart contracts, a permissioned EOS blockchain, resource providers, and distant users make up this system. We just installed and tested one data-sharing smart contract in order to keep things straightforward. To successfully send data, each resource owner needs to implement a number of smart contracts, though. Using the distant users' public keys, the resource owner may add, update, or remove data sharing policies.Each remote user sends an access request for the data stored in IPFS using a client application in order to access the data owned by the resource owner. The permissions field in the data sharing policy is used by the data sharing smart contract to determine whether to grant or deny a request. The key elements of our suggested architecture are covered in this section.A. Smart Agriculture: This type of agriculture uses a variety of Internet of Things sensors, including light, water level, actuators and humidity. The idea of "smart farming" is still in its infancy because of IoT devices that can provide data about farmers' agricultural lands. A computer or mobile device is used by the owner of each agricultural field to administer it. The owner of the data made in the agricultural sector decides who can use it.B. Interplenary File System (IPFS): The P2P distributed file system known as IPFS is currently referred to as the "backbone of the Third Web." Hash values are used to uniquely identify files stored in the IPFS. These hashes are used to develop data sharing rules for the blockchain.Before being transmitted to IPFS for storage, data generated by IoT devices for smart agriculture is encrypted. The resource owner delivers a transfer of cash to the data sharing smart contract, as shown in Fig. 2, to distribute data using its hash. To offer users services, IPFS nodes are interconnected with thousands of other nodes. IPFS uses techniques like BitTorrent and the Distributed Hash Table (DHT) to build a P2P file system. It is a special file system created to deal with the problems that IoT devices have with authentication, dependability, stability, and sustainability.In contrast to the client-server architecture, IPFS's safe and encrypted filesharing technology enables secure data transit among peers. Blockchain technology's IPFS is a foundational component [16]. In order to achieve safe data sharing in IoT-based smart agriculture, IPFS is the perfect storage and sharing platform.C. Smart Contract: To facilitate data sharing for the resource owner, the data sharing smart contract incorporates access control. It is built on ACLs and allows for the creation of simple, granular data sharing rules that require less blockchain storage. The data sharing guidelines in Fig. 1 show how Access Control Lists enable the resource owner to exchange data with a certain group of people.It is crucial to remember that IoT device can use access control strategy of the data sharing smart contract to lookup permissions inside the blockchain.

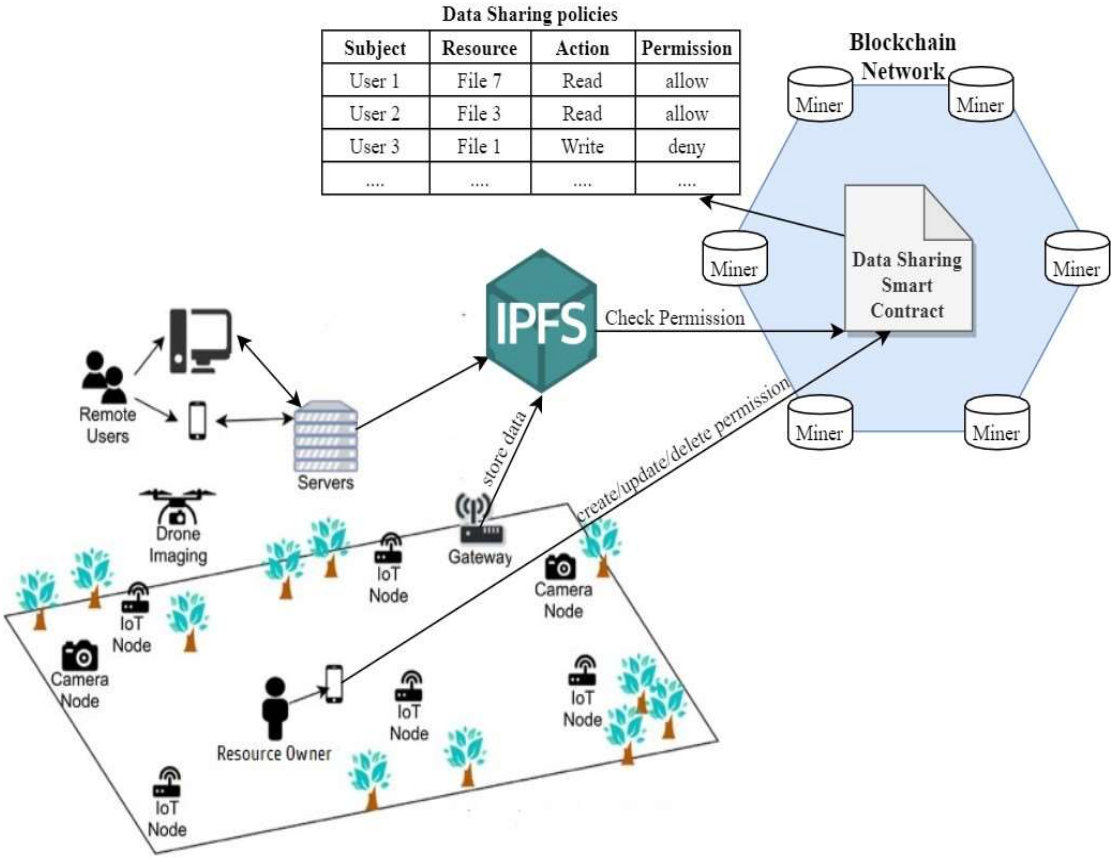


Fig. 1 The blockchain-based data-sharing infrastructure for smart agriculture is shown in broad strokes.

D. Server: To offer users smart agriculture services, a server is a device that can interface with Internet of things andIPFS devices. These interactions include data collection from the IPFS, data storage in the IPFS, and data retrieval from the IPFS.
E. Distant Users: Distant users can read and write to the shared data on the servers, based on the rules that the resource owner has set up on the blockchain for sharing data.
F. User Device: Each user in a different place can change the data using a device, like a laptop, PC, or smart phone.
G. IoT Gateway: Using several communication methods, including ZigBee and Wi-Fi, the Internet of things gateway connects smart agriculture with the P2P IPFS storage device.

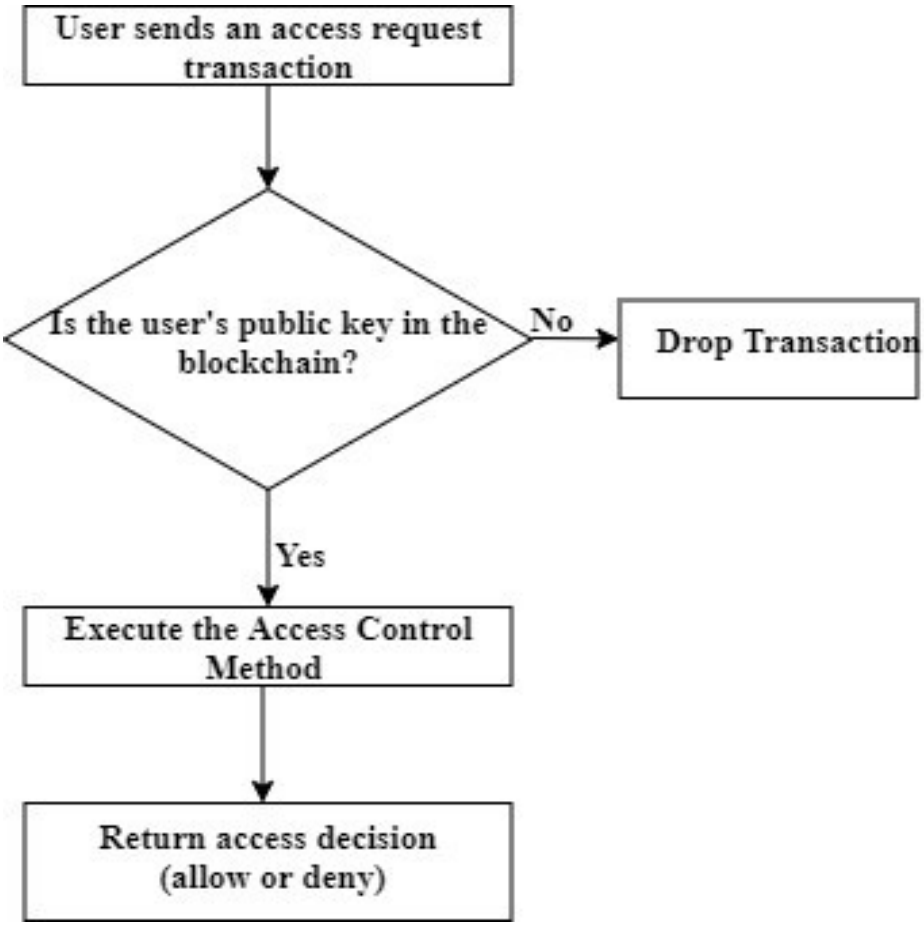


Figure 2 shows the proposed system's flowchart after an access request transaction.

A basic flowchart of the suggested system is shown in Fig. 2.Every time a user submits an access control transaction, the IPFS communicates with the information smart contract to verify accessibility authorization on the blockchain.The blockchain first validates the existence of the requiring user's public key. In the absence of a key, this transaction is cancelled. If not, the data sharing smart contract implements the access control mechanism using the receiving user's decryption key as an input argument. After that, the smart contract sends a formal request, informing the user whether or not the requested action is permitted.

IV. ANALYSIS AND EVALUATION

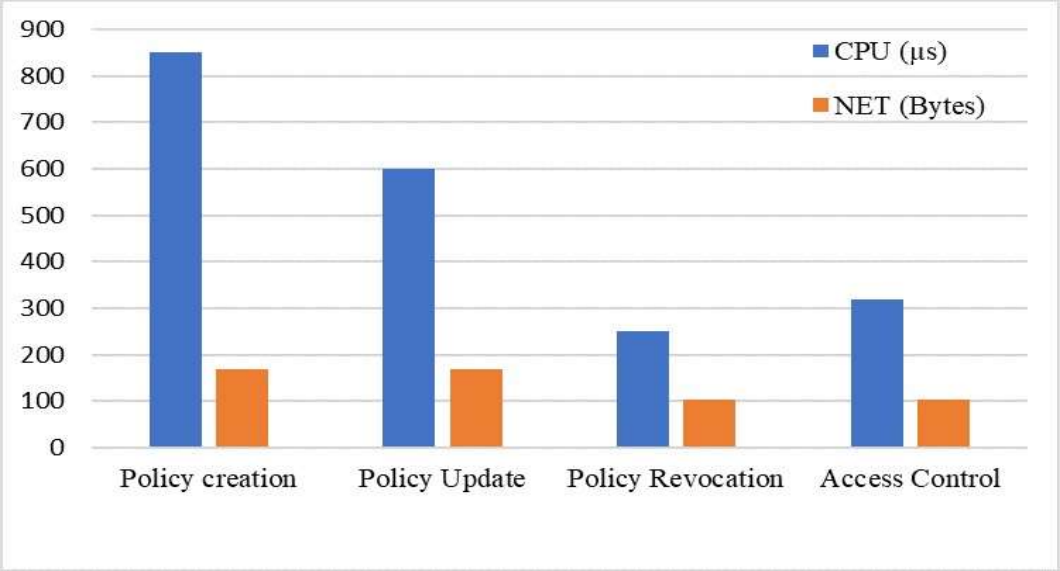
A. Security Analysis

Confidentiality, integrity, and availability, or CIA, are the three main security needs that must be addressed by a data sharing system that integrates access control [17]. Because of the need for confidentiality, only an authorised user will be able to access and modify the data.Integrity makes sure that only allowed changes are made to the data. Finally, availability guarantees that users will always have access to the data when needed. Due to blockchain's persistency feature,

our suggested approach guarantees availability and integrity. It is never possible to erase or edit data once it has been written to the blockchain (except by the resource owner). As a result, our blockchain-based solution offers a constantly accessible atmosphere that enables the storage device to have tamper-proof proof of the blockchain's policies. Additionally, EOS smart contracts feature unique modifiers that allow them to only accept transactions for the creation, modification, and revocation of policies from the resource owner.Denial of Service (DoS) attacks can be used against agriculture solutions now in use that are based on a central server. For instance, Chen et al.'s central server is used to store agricultural data. To prevent users from accessing the data, an attacker may easily launch a DoS attack on the server. However, our suggested method offers resistance to DoS assaults.

B. **Analysis of Performance**

The data-sharing smart contract on the EOS blockchain system was developed, installed, and tested using the C++ programming language. EOS provides the contract development tools (CDT) for creating and testing smart contracts [6].
Contract development tools changes the contract source code to Web Assembly syntax so that it can be used in the EOS virtual machine.
By including the subjects' public keys in transactions sent to the data exchange smart contract that is accessible on the EOS blockchain, resource owners can modify,and delete data sharing rules, and create. Depending on how complicated they are, these transactions need a certain amount of resources. Computational power and network connectivity, also known as NET and CPU, are the two resource types that EOS requires. The data exchange smart contract's running costs are shown in Fig. 3 and were made available to the public on the EOS blockchain. The person who owns the copyright sends a policy creation transaction to the user so that they can share farm data with them. The owner of the resource may at any moment edit the permission field to grant or restrictaccess. Compared to other transactions, this one uses more CPU resources.The resource, action, and permission fields of a current policy are changed by the policy upgrade operation. The resource owner can cancel a policy at any moment by publishing a policy withdrawal transaction to the blockchain. The copyright holder can cancel a policy at any moment by uploading a policy withdrawal transaction to the blockchain.The areas inside the data sharing standards are also taken into consideration by the access control system when determining whether or not to grant requests for access. Table I compares the three widely used blockchain platforms' average transaction costs [18]. The data show that when it comes to average transaction prices, Ethereum is the most expensive. Transaction costs are a significant issue for stakeholders in agriculture, as was already mentioned.



The operational costs of the smart contract for data sharing are shown in Fig. 3.

Steller	EOS	Ethereum	Cost Type
0.00005300	Nullpayment	0.12	End250 blocks
0.00000141	Nullpayment	0.72	Mainnet (USD)

TABLE I: The average transaction costs for the ETH, Stellar, and EOS blockchains

Table II demonstrates how the EOS blockchain could change current IoT applications [19], [18].

Steller	EOS	Ethereum	Features
3.3	74.84	19.4	Throughput
No	Yes	No	Private Transactions
5 sec	0.5 sec	10-19 sec	Block Production Rate
Limited	Unlimited	Limited	Scalability
30 sec	1 sec	1 min	Confirmation Time
Any	Any	Solidity	Languages
Limited	Yes	Yes	Smart Contract

Comparative Analysis of Blockchain Platforms in Table II

V. Conclusion

This paper analyses the primary challenges that Internet of Things-based smart agriculture faces in order to meet stakeholder expectations. It then suggests a better, distributed data sharing technique that uses a developing smart contract platform.The Interplanetary File System (IPFS), smart contracts, smart agriculture, and agriculture stakeholders make up the four levels of our system's design. In contrast to the client-server architecture, IPFS's safe and encrypted filesharing technology enables secure data transit among peers. The blockchain's data sharing smart contract is used by the resource owner to add, remove, or modify data sharing policies. Using smartphones, laptops, or PCs, remote users make changes to the shared data. To protect consumers' privacy, our method employs anonymous identities. Important security needs, including confidentiality, integrity, and availability, are satisfactorily met by our system.So far as we know, this study is the first to try to make a smart agriculture data-sharing system that will last. To address other IoT problems, we will create smart contracts in our upcoming research.

References:

[1] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, “Internet ofthings in agriculture, recent advances and future challenges,” BiosystemsEngineering, vol. 164, pp. 31–48, 2017.

[2] D. Chen, B. Wu, T. Chen, and J. Dong, “Development of distributeddata sharing platform for multi-source iot sensor data of agricultureand forestry,” Transactions of the Chinese Society of AgriculturalEngineering, vol. 33, no. 1, pp. 300–307, 2017.

[3] Y.-P. Lin, J. R. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F.Chou, and Y.-F. Ho, “Blockchain: The evolutionary next step for icte-agriculture,” Environments, vol. 4, no. 3, p. 50, 2017.

[4] pEOS Whitepaper, “Private, untraceable transactions on eos,” 2019. [Online]. Available: ,https://pEOS.one/docs/pEOS whitepaper rev1 1.pdf[5] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, “Blockchainand scalability,” in 2018 IEEE International Conference on SoftwareQuality, Reliability and Security Companion (QRS-C). IEEE, 2018,pp. 122–128.

[6] D. Macrinici, C. Cartofeanu, and S. Gao, “Smart contract applicationswithin blockchain technology: A systematic mapping study,” Telematicsand Informatics, vol. 35, no. 8, pp. 2337–2354, 2018.

[7] Pathak, N., Siddiqui, S. T., Singha, A. K., Mohamed, H. G., Urooj, S., &Patil, A. R. (2023). Smart Quarantine Environment Privacy through IoT Gadgets Using Blockchain. Intelligent Automation & Soft Computing, 35(3).

[8] B. Xu, D. Luthra, Z. Cole, and N. Blakely, "Eos: An architectural,performance, and economic analysis," Retrieved June, vol. 11, p. 2019,2018.

[9] L. Hang, I. Ullah, and D.-H. Kim, "A secure fish farm platform basedon blockchain for agriculture data integrity," Computers and Electronicsin Agriculture, vol. 170, p. 105251, 2020.

[10] L. Ge, C. Brewster, J. Spek, A. Smeenk, J. Top, F. van Diepen, B. Klaase,C. Graumans, and M. d. R. de Wildt, Blockchain for agriculture andfood: Findings from the pilot study. Wageningen Economic Research,

2017, no. 2017-112.

[11] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Securityand privacy for green iot-based agriculture: Review, blockchain solutions, and challenges," IEEE Access, vol. 8, pp. 32 031–32 053, 2020.

[12] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis,A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al.,"Hyperledger fabric: a distributed operating system for permissionedblockchains," in Proceedings of the thirteenth EuroSys conference, 2018,pp. 1–15.

[13] E. Jakku, B. Taylor, A. Fleming, C. Mason, S. Fielke, C. Sounness, andP. Thorburn, ""if they don't tell us what they do with it, why would wetrust them?" trust, transparency and benefit-sharing in smart farming,"NJAS-Wageningen Journal of Life Sciences, vol. 90, p. 100285, 2019.[14] M. S. Devi, R. Suguna, A. S. Joshi, and R. A. Bagate, "Design of iotblockchain based smart agriculture for enlightening safety and security,"in International Conference on Emerging Technologies in ComputerEngineering. Springer, 2019, pp. 7–19.

[15] Y. Voutos, G. Drakopoulos, and P. Mylonas, "Smart agriculture: Anopen field for smart contracts," in 2019 4th South-East Europe DesignAutomation, Computer Engineering, Computer Networks and SocialMedia Conference (SEEDA-CECNSM). IEEE, 2019, pp. 1–6.[16] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXivpreprint arXiv:1407.3561, 2014.

[17] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid andsmart home security: Issues, challenges and countermeasures," IEEECommunications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954,

2014.

[18] I. Mokdad and N. M. Hewahi, "Empirical evaluation of blockchain smartcontracts," in Decentralised Internet of Things. Springer, 2020, pp. 45–71.

[19] M. Garriga, M. Arias, and A. De Renzis, "Blockchain and cryptocurrency: a comparative framework of the main architectural drivers," arXivpreprint arXiv:1812.08806, 2018.

[20]Zubair, S., Singha, A. K., Pathak, N., Sharma, N., Urooj, S., &Larguech, S. R. (2023). Performance Enhancement of Adaptive Neural Networks Based on Learning Rate. CMC-COMPUTERS MATERIALS & CONTINUA, 74(1), 2005-2019.

[21]Singha, A. K., Pathak, N., Sharma, N., Tiwari, P. K., & Joel, J. P. C. (2023). COVID-19 Disease Classification Model Using Deep Dense Convolutional Neural Networks. In Emerging Technologies in Data Mining and Information Security (pp. 671-682). Springer, Singapore.

[22]Singha, A. K., Pathak, N., Sharma, N., Tiwari, P. K., & Joel, J. P. C. (2023). Forecasting COVID-19 Confirmed Cases in China Using an Optimization Method. In Emerging Technologies in Data Mining and Information Security (pp. 683-695). Springer, Singapore.

[23]Siddiqui, S. T., Ahmad, M. O., Khamruddin, M., Gupta, A. K., & Singha, A. K. (2022, January). Blockchain and IoT for Educational Certificates Generation and Verification. In 2022 2nd International Conference on Computing and Information Technology (ICCIT) (pp. 298-303). IEEE.