Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Farmer Online Shopping for Buying and Selling

A. Sunitha[1], P. Pavani[2], K. Sreenath[3], R. Sarala[4], P. Shobha Rani[5]

[1,2,3,4,5]Department Of CSE, Tadipatri Engineering College , Tadipatri.

Abstract

Blockchain is growing as a potential force capable of changing the financial services industry by making the fund transfer immediate, cheaper and more secure. Current existing system is not secure enough to give 100% fraud protection because of more manual work and lack of security of data. Blockchain is nothing but a chain made of blocks (nodes).These process node does the all major work. These blocks are connected to each other using cryptography. This system will be more expeditious, more efficient, and has user affectional interfaces in the banking and has zero probability of losing data while processing of the user data. In integration to enabling trade, block chain is larceny-and tamper-resistant model, it eliminates errors and the duplication, blockchain is ideal for reserving the data in blocks and using a tamper-proof hash format, so the data can be securely stored by bank and make the current existing system much more secure and faster. Which is already done in case of cryptocurrency.

Keywords: Blockchain, Cryptograph, Tagging Farm, Cryptocurrency, AES - advanced encryption standard, DES - data encryption standard.

INTRODUCTION

Blockchain is digital, distributed and public ledger. Blockchain technology was first used in now a days popular cryptocurrency called BITCOIN (virtual currency), but it is expected that its characteristics of accurate and guarded data transfer in distributed P2P network could make other applications possible. In blockchain nodes are connected cryptographically and in chronological order. The blockchain offers ability to distribute ledgers in decentralized way and that's a key concept. Unlike centralized system where the ledgers of records are stored in single specific entity like a bank or governmental institution, the blockchain shares the ledgers in between its participants [1]. That's what make blockchain decentralized. This means that ledgers are written and stored in network and its members are responsible to update and monitor it. Every block of record is constantly synchronized by the different members of the open network, creating multiple copies of the data through a shared record-keeping system ensuring no single person or an organization holds ownership of data. When an incipient transaction or an edit to a subsisting transaction comes in to a blockchain, generally a most of the nodes within a blockchain implementation have to apply steps (algorithm) to calculate and validate and verify the past of the individual block chain's block that is introduced. When all the node come to an agreement or consensus that history and signature of the transaction is valid then that new particular block is then added to chain of the transaction [2]. If a majority of nodes does not agree to the integration in ledger ingression then block is not added to chain. This kind of working allows this blockchain methodology to run without any need of central authority. In blockchain each block contain number of transactions. It provides a decentralized, immutable data store that can be used across a network of users, engenders assets and acts as a shared ebony book that records

all transactions. So, a blockchain establishes an auditable and indisputable open record of information that is cheaper, faster and more secure than any other centralized system.

That make blockchain decentralized. This implies that records are composed and put away in every record block is constantly being updated and monitored by the network and its members. Synchronized by the different individuals from the open organization, making various duplicates of the information through a shared record-keeping system that ensures that neither an individual nor an organization owns data. When an a blockchain receives an incipient transaction or an edit to an existing transaction, typically most hubs inside a blockchain execution need to apply steps (calculation) to compute and approve and confirm the preceding block of the particular blockchain that is introduced. When all of the nodes reach a consensus or agreement that set of experiences and mark of the exchange is legitimate then that new particular block is then added to chain of the exchange. On the off chance that a larger part of hubs doesn't consent to the mix in record ingression then, at that point, chain does not include a block. This way of working makes it possible for the blockchain methodology to operate without centralized control in blockchain each block contains number of exchanges. It gives a decentralized, unchanging information store that can be utilized across an organization of clients, incites resources and goes about as a common dark book that records all exchanges. Thus, a blockchain lays out an auditable and unquestionable open record of information that, in comparison to any other centralized system, is more secure, faster, and cheaper.

LITERATURE ANALYSIS

One of the most important steps in the software development process is the literature review. Determining the time component, cost savings, and commercial business robustness is essential before expanding the gadget. After these are satisfied, the next stage is to identify the language and operating device that can be utilized to expand the device. Programmers require a lot of outside assistance once they begin building a device. This assistance can be obtained via websites, books, or senior programmers. The aforementioned issues are taken into account when constructing the system in order to expand the suggested device.

Examining and reviewing all of the challenge improvement's needs is the core function of the assignment improvement department. Literature evaluation is the most crucial stage in the software development process for any task. Prior to expanding the equipment and associated layout, time considerations, resource requirements, labor, economics, and organizational electricity must be identified and evaluated. The next phase is to determine the operating system needed for the project, the software program specifications of the particular computer, and any software that needs to be carried on after those factors have been met and thoroughly investigated. a stage similar to expanding the tools and related capabilities.

In [1] in terms of stability, we discover and address a few gaps (the quantity to which keyword searches produce fake positives) for public key encryption. (PEKS). We outline statistical and computational extensions of the modern idea of best balance, show that the Eurocrypt 2004 scheme of Bone et al. Is computationally comfortable, and we recommend a new statistically superior stability scheme. In addition, we offer a at ease transition to the nameless IBE software. Unlike preceding initiatives, the PEKS challenge ensures balance. Finally, we endorse three extensions to the fundamental ideas mentioned here, together with anonymous HIBE, public-key identity-based totally encryption with time-based keyword seek, and key-word search encryption. In [2] atom became proposed by means of Blaise, Blymer, and Strauss (BBS) in 1998. Proxy re-encryption, in which a distinctly trusted proxy converts Alice's cipher text into Bob's cipher text without seeing the underlying plaintext. We assume fast and cozy re-encryption to become a common method for managing encrypted record systems. Although smooth to recognize,

numerous protection worries have avoided big attractiveness of the dangers associated with BBS re-encryption. We present a new re-encoding that follows on from current paintings by way of Toddies and Ivan. We reveal the software of using proxy re-encryption to control who can get admission to at ease garage system and the schemes that implement the robust protection concept. Performance assessments on our take a look at report device demonstrate the realistic reliability of proxy re-encryption.

The machine "Public Key Encryption Keyword Search" (PEKS) advanced by using Bone, Di Crescenzo, Ostrovsky, and Persiano permits to encrypt search key phrases without compromising the security of the authentic statistics. In this paper, we deal with predominant problems of the PEKS scheme, "relaxed channel elimination" and "key-word update", which Bone et al. Did no longer cope with in this paper. We locate that the usage of a secure channel makes the unique PEKS scheme inefficient. We develop a green PEKS scheme to address this issue of doing away with secure connectivity. We accept as true with that warning must be taken in thinking about the opportunity that this example may be incompatible with the security of PEKS [3]. In [4] Cloud computing has made a shared set of resources to be had to curious about multiple gamers and partners in the e-fitness zone. Outsourcing data has unavoidably caused a rapid increase in cloud computing safety issues. The security of cellular gadgets is compromised through their restrained sources. To permit this, solutions want to transport the entire computing method to the cloud. Typically, any modifications to the loaded record might force the mobile customer to fully encrypt and recomputed the hash fee. In this paper, we plan to recommend a sturdy, pair less intermediate scheme for re-encryption that works proportionally to the wide variety of adjustments made over the years instead of the report length, which should be optimized in document conversion responsibilities. The proposed scheme shows upgrades within the strength consumption and rotation timer length of the file conversion device. By a, the proposed scheme is verified via a systematic method applied the usage of the Z3 solver. In [5] physicians can use good sized, speedy get admission to to non-public scientific information to make vital selections and store lives. Cloud computing gives instant, on-call for get admission to a hard and fast of shared sources and digital services to diverse stakeholders inside the e-fitness zone, together with sufferers, healthcare providers, insurers, and others. Furthermore, the mixing of cloud computing into digital fitness systems increases concerns approximately a wide variety of safety issues associated with facts outsourcing. Therefore, the cryptographic evaluation of the QIN mission is executed by way of violating their privacy plan. We additionally advise a lightweight, compliant, one-manner, certificates-unfastened, unmarried-hop elliptic curve re-encryption scheme for securely sharing mobile personal fitness records with an efficient public cloud for low-electricity cellular devices. Patients can use proxy certificate less re-encryption to encrypt statistics using their public keys and outsource it to the cloud and use the cloud. The semi-relied on resident proxy, without understanding something about the recipient's public key, re-encrypts the encrypted message returned into the cipher text as expected. We demonstrate its security by means of conducting systematic checking out against a specific cipher text attack on a random oracle pattern, and our proposed method could be very effective compared to existing schemes and is suitable for low-energy cell devices [5].

The automatic detection of pancreatic tumors is this system's primary goal. The widespread use of contrast-enhanced computed tomography (CT) for pancreatic cancer staging and diagnosis only traditional methods made by hand extract features at a low level. However, normal convolutional neural networks are unable to make full use of relevant context data, which leads to poor detection results. A novel and effective pancreatic tumor detection framework is presented in this paper designed with the goal of fully utilizing the context data across multiple scales.

PROPOSED ARCHITECTURE

The user is the main module that makes up the system. Users can register as distributors, retailers, manufacturers, farmers, and consumers. They can use their login information to log in. They are able to see their profile. If they so choose, they can even alter the password. The items can only be managed by farmers and manufacturers. The products that the user needs are added, updated, and viewed. They can even use filters to look for things. Products in the entry product list are viewable and addable by the user. They can even use filters to look for the listings. They can see every piece of the supply chain. By selecting items from the entering product list, the user can view or add items to the exit product list. They are even able to assign the clients to the merchandise. They can even use filters to look for the list of exit products. They can see every piece of the supply chain. Products in the Used Today category can only be added or viewed by retailers and consumers. From the entry-level product list, they can select the items they want. They can use filters to look for the list as well. They can see every piece of the supply chain. Additionally, the user can monitor their diet. They can also look into the supply chain and history. HTML, CSS, and JavaScript make up the front end of this system, while ASP.net and C# make up the back end. Visual Studio is the IDE while MSSQL is the database.

SELECTED METHODODLOGIES

Blockchain: Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, and land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. Business runs on information. The faster information is received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared, and observable information that is stored on an immutable ledger that only permissioned network members can access. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, and new efficiencies and opportunities.

AES - advanced encryption standard: An extremely reliable encryption algorithm called Advanced Encryption Standard (AES) is used to protect data by transforming it into a format that cannot be read without the right key. The National Institute of Standards and Technology (NIST) created it in 2001. Despite being more difficult to install, it is nevertheless extensively used today since it is far more powerful than DES and triple DES. AES encryption offers robust defense against unwanted access by utilizing several key lengths (128, 192, or 256 bits). This data security strategy is effective and frequently used to encrypt files, safeguard sensitive data, and secure internet connection. AES, a key component of contemporary encryption, is well known throughout the world for its capacity to protect data from online attacks.

DES - data encryption standard: The Data Encryption Standard (DES), a well-known encryption technique with a 56-bit key length, is discussed in this article. We examine how it works, how keys are changed, and how encryption works, illuminating both its function in data security and its shortcomings in the modern world. Data security has benefited greatly from the use of the 56-bit key length block cipher known as the Data Encryption Standard (DES). Due to its vulnerability to extremely potent assaults, the Data Encryption Standard (DES) has seen a minor fall in usage. DES is a block cipher that encrypts data in blocks of 64 bits each. When 64 bits of plain text are fed into DES, 64 bits of cipher text are generated.

With a few minor variations, the encryption and decryption processes use the same algorithm and key. The length of the key is 56 bits.

SYSTEM ARCHITECTURE

The portrayal of the general characteristics of the product is connected to the meaning of the prerequisites and the laid-out request of a serious level of the contraption. Numerous web pages and their connections are described and designed during architectural design. Key software components are defined, broken down into processing modules and conceptual records systems, and the connections that exist between them are explained. The proposed framework characterizes the accompanying modules. The user is the main module that makes up the system. Users can register as distributors, retailers, manufacturers, farmers, and consumers. They can use their login information to log in. They are able to see their profile. If they so choose, they can even alter the password. The items can only be managed by farmers and manufacturers. The products that the user needs are added, updated, and viewed. They can even use filters to look for things. Products in the entry product list are viewable and addable by the user. They can even use filters to look for the listings. They can see every piece of the supply chain. By selecting items from the entering product list, the user can view or add items to the exit product list. They are even able to assign the clients to the merchandise. They can even use filters to look for the list of exit products. They can see every piece of the supply chain. Products in the Used Today category can only be added or viewed by retailers and consumers. From the entry-level product list, they can select the items they want. They can use filters to look for the list as well.

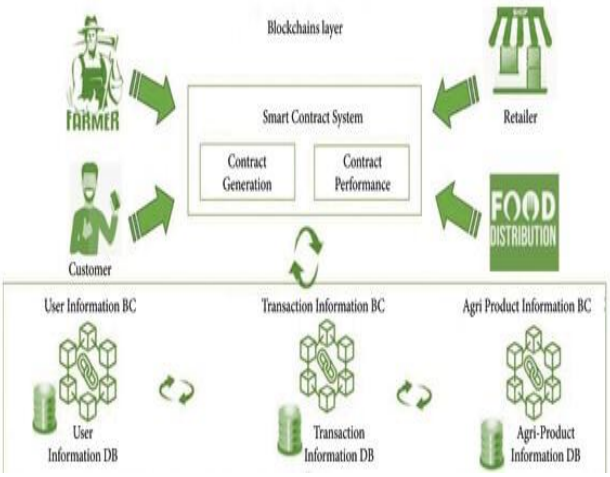

Fig 1: System Architecture

SYSTEM MODULES

a) Acquirer Settlement Bank (Merchant's Bank)

- **Login**

Login to the system

- **Merchants List**

Every merchant listed with the information of the service period.

- **Merchant's Transactions**

A list of every merchant transaction (for bank services) that includes the status of any tempered or altered

transactions.

- **Notification**

The merchant will receive a notification from the bank to renew services.

- **Renew Agreement**

The bank may extend the service agreement for the appropriate time frame.

- **Fee Transactions**

All customer transactions will have their charges per transaction listed.

b) Merchant

- **Login**

Login to the system.

- **My Profile**

Change Password

- **Home Page**

Enter your account details to connect to the bank and view the service period (Expiry date).

- **Service Transaction**

A bank account can be used by the merchant to pay for services.

- **View Transactions**

This module lists all of the transactions the merchant has made for services, along with the status of any tempered or altered transactions.

- **Customers Transactions**

Here, every customer transaction will be shown, along with the status of any tempered or altered transactions.

- **Customers Details**

All Customers list.

- **Notification**

The bank's notification will be displayed.

- **Renew Agreement**

The merchant can send the agreement's approval.

- **View Feedback**

Customers Feedback list.

c) Customer

- **Register**

Register by filling in details.

- **Login**

Log in to the system.

- **My Profile**

Customer’s registered details.

Change Password

- **Merchant List**

All Merchants Listed in this module.

- **New Transaction**

Proceed with processing the transaction for a particular merchant. However, the acquirer's (admin) account

is used for the actual transaction.

- **View Transaction**

All of the customer's transactions will be shown here, along with the status of any tempered or altered transactions.

- **Feedback**

Customers are able to share their system-using experiences.

RESULT & DISCUSSION

Using a blockchain application to tag farm products guarantees agricultural trade's efficiency, security, and transparency. The method effectively removes middlemen, allowing farmers (sellers) and purchasers to trade directly while keeping an unchangeable record of every transaction. Blockchain technology improves data security and integrity while lowering the possibility of fraud and manipulation. By automating payment processing, smart contract integration makes sure that transactions are only completed when certain requirements are satisfied. When compared to older systems, performance evaluations show that transaction processing is effective and has few delays. However, issues like network latency, blockchain scalability, and early adoption difficulties for farmers who are not familiar with the technology must be resolved. All things considered, the suggested solution increases stakeholder trust, guarantees farmers fair prices, and gives consumers genuine, traceable agricultural products.

SCREENSHOTS

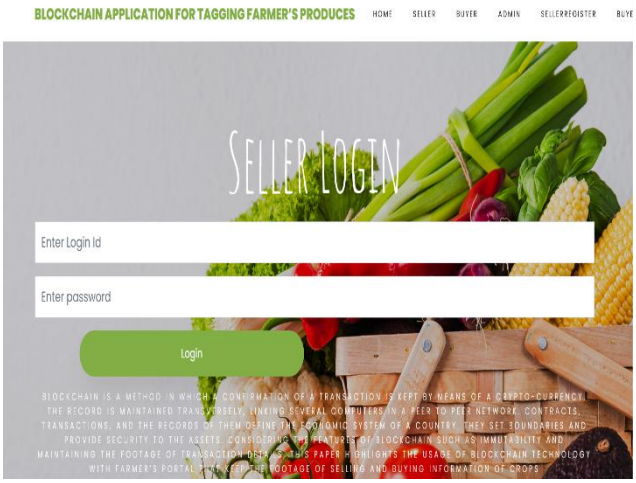

Fig 2: Login Page

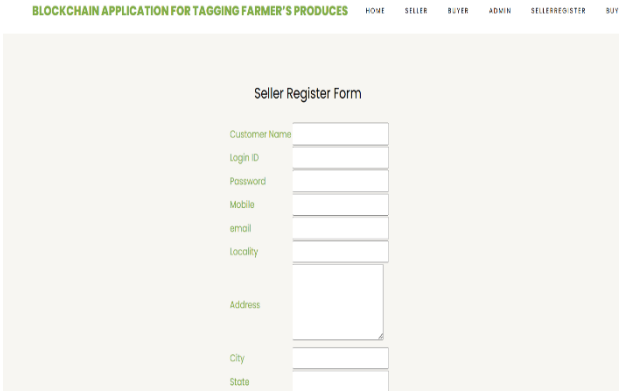

Fig 3: Register Page

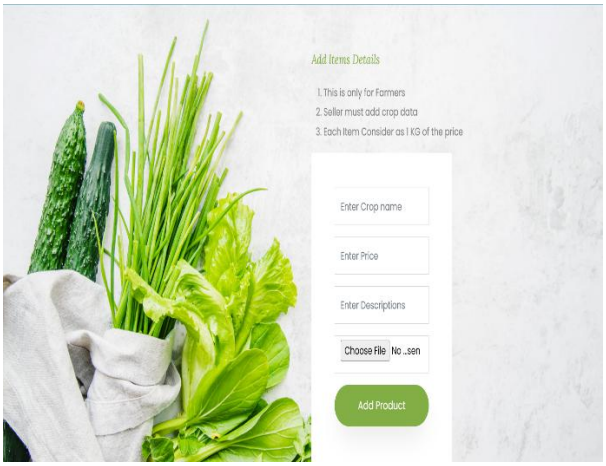

Fig 4: Home Page

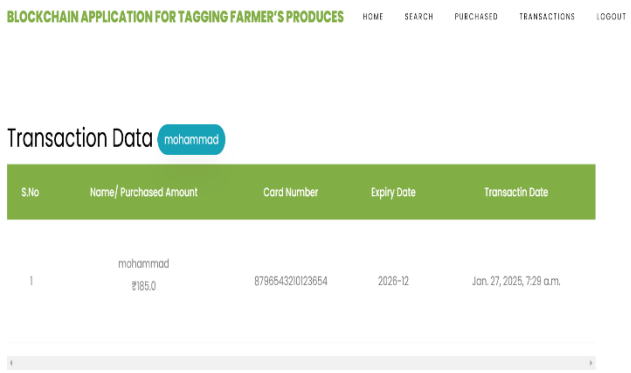

Fig 5: transaction page

CONCLUSION

The article concludes that, further to the continuation of extensive issues with the centralized control of the device and the involvement of a public derivative system contract, the operation of the trade device within the out of date gadget has evolved over many years, which has been evolved and changed taking into consideration the blockchain foundations to begin with advanced, however serves as an unconditional device for growing a corruption-loose environment. A tremendous option to this trouble is a blockchain-based totally transaction gadget. Each new change inside the blockchain simplifies matters, solves essential troubles, and makes peer-to-peer sharing possible.

FUTURE SCOPE

Cybersecurity is the main future path of blockchain technology. Despite the open and distributed nature of the Blockchain system, data is still safe and verifiable. Data is encrypted using cryptography, which removes security vulnerabilities like illegal data manipulation. Blockchain employment is currently one of the most talked-about strategies among companies and is propelling the expansion of the IT industry. Thus, blockchain technology offers tremendous potential for those who possess the necessary abilities and expertise. In multicomponent transactions that need verification and traceability, it may be helpful for validation and traceability. Additionally, it facilitates safe transactions, lowers compliance costs, and expedites data transfer processing. It also helps with audits of product provenance and contract

management. Because of the large number of applicants, it provides a selection of job descriptions to fit your interests and qualifications.

.

REFERENCES

1. X. Zhang, P. Sun, J. Xu, X. Wang, J. Yu, Z. Zhao, and Y. Dong, ‘‘Blockchain-based safety management system for the grain supply chain,’’ IEEE Access, vol. 8, pp. 36398–36410, 2020.
2. A. Vangala, A. K. Das, N. Kumar, and M. Alazab, ‘‘Smart secure sensing for IoT-based agriculture: Blockchain perspective,’’ IEEE Sensors J., early access, Jul. 27, 2020, doi: 10.1109/JSEN.2020.3012294.
3. N. Bore, A. Kinai, P. Waweru, I. Wambugu, J. Mutahi, E. Kemunto, R. Bryant, and K. Weldemariam, ‘‘ADW: Blockchain-enabled small- scale farm digitization,’’ 2020, arXiv:2003.06862. [Online]. Available: http://arxiv.org/abs/2003.06862
4. I. A. Omar, R. Jayaraman, K. Salah, M. Debe, and M. Omar, ‘‘Enhancing vendor managed inventory supply chain operations using blockchain smart contracts,’’ IEEE Access, vol. 8, pp. 182704–182719, 2020.
5. H. Zhang, E. Deng, H. Zhu, and Z. Cao, ‘‘Smart contract for secure billing in ride-hailing service via blockchain,’’ Peer-Peer Netw. Appl., vol. 12, no. 5, pp. 1346–1357, Sep. 2019.
6. S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, ‘‘An incentive mechanism for data sharing based on blockchain with smart contracts,’’ Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106587.
7. A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, ‘‘Blockchain-based agri-food supply chain: A complete solu- tion,’’ IEEE Access, vol. 8, pp. 69230–69243, 2020.
8. Z. Yu, D. Xue, J. Fan, and C. Guo, ‘‘DNSTSM: DNS cache resources trusted sharing model based on consortium blockchain,’’ IEEE Access, vol. 8, pp. 13640–13650, 2020.
9. X. Li, F. Lv, F. Xiang, Z. Sun, and Z. Sun, ‘‘Research on key technologies of logistics information traceability model based on consortium chain,’’ IEEE Access, vol. 8, pp. 69754–69762, 2020.
10. H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, ‘‘BDSS-FA: A blockchain- based data security sharing platform with fine-grained access control,’’ IEEE Access, vol. 8, pp. 87552–87561, 2020.