IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Government Fund Allocation Using Blockchain

Jay Jagtap[1], Pradhumna Jadhav[2,] Rushikesh Wanjale[3], Ninad Mane[4], Mrs. Hema Kumbhar[5]

U.G. Student, Department of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India[1,2,3,4]

Project Guide, Department of Computer Engineer, RMD Sinhgad School of Engineering, Maharashtra, India[5]

ABSTRACT:

Governments need to cater to a huge number of responsibilities of a state. The working of state governments involves huge number of transactions towards various operations that need to be carried out throughout the state. This includes new projects, repair and maintenance works, awarding contracts, paying of government employees, farmer schemes and so on. A major obstacle that the top government face is the low level corruption that is sometimes not possible to track which deprives the state progress. Tracking it is a very complicated task due to the current system. But in proposed system we overcome this drawbacks by using block chain approach. We here make use of blockchain technology to secure the transactions at every stage while maintaining transparency in every transaction sealing every transaction with proofs as the funds move ahead. Blockchain is an evolving technology that maintains a chain of records known as blocks, connected through cryptography. Each block contains a unique identifier (cryptographic hash) of the previous block, a timestamp, and transaction data. The inherent design of a blockchain ensures that the data stored within it is highly resistant to unauthorized modifications. The proposed system focuses on enabling the tracking of funds allocated to the government throughout the entire allocation process. To ensure secure communication, key pair generation algorithms will be employed, enabling the establishment of trusted channels between relevant entities involved in fund allocation. Key pairs consist of a public key for secure data sharing and a private key for authentication and decryption. Moreover, metadata file decryption algorithms will be used to securely decrypt encrypted metadata associated with fund allocation transactions. This process allows authorized entities to verify transaction details, contributing to a higher level of transparency in the fund allocation process. Additionally, data verification algorithms will be implemented to ensure the integrity and authenticity of data stored within the blockchain. These algorithms play a crucial role in preventing unauthorized modifications to the blockchain records, preserving the immutability of the data

By combining these proposed algorithms and harnessing the power of blockchain technology, this project aims to enhance the security, transparency, and integrity of government fund allocation. The utilization of key pair generation, metadata file decryption, and data verification algorithms enables efficient and accountable fund allocation within the government system.

KEYWORDS: Block chain, HyperLedger, Security, Transparency, Encryption, Government Funds, Cryptography, AES.

INTRODUCTION:

Overview

India, the world's fastest expanding economy, has a lot of promise in terms of drawing international customers and adapting to new technology and developments. Digitalization offers a lot of potential for improving and enhancing connectivity in almost every sector of the economy. However, the distribution of these approaches is sometimes uneven within a few government sectors. Adapting to the newest evolving technology will, in turn, assist in providing excellent value and a significant shift in the mode of operations/work for a broad group of individuals. One such technology is blockchain. It is being used by every sector in the world due to its features such as decentralized method, secure, unchangeable, and tamper-proof nature. In India, on the other hand, funds are a hot topic, with numerous public-interest programmers receiving massive sums of money as funds. Due to a lack of transparency, Blockchain can be utilized to fill the void and create a fully secure, immutable environment for tracking funds.

The ability of blockchain to improve the trust and transparency of information-based trades between people and organizations has been lauded. When used in the right circumstances, the innovation provides assurance. Typically, organizations with their own, separate IT systems attempting to collaborate face challenges such as data compromise, identifying a single source of truth, and encouraging accountability. Blockchain technology addresses these issues by providing a specific foundation that enables the execution of shared business forms in such a way that no single substance has authority over the entire system. The need for government to collect, support, and promote open trust in data and frameworks is a common one. In some cases, blockchain technology may be able to aid in the improvement of trust.

Motivation

- Nowadays blockchain is emerging technology, its feature like decentralized approach, secure, immutable, tamper proof nature it is being adopted by each and every sector globally.
- Funds in India, on the contrary, is a heated topic and various schemes issued in public interest are allotted tons of money as funds
- .Due to the lack of transparency, Blockchain can be used to bridge that gap and to provide the fully secure, immutable environment for funds tracking.

RELATED WORKS :

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and
start working with the reference of previous papers. In this section, we review improving the Security Levels of e-Government Processes within Public Administration through the Establishment of Improved Security Systems.

Stavros Zouridis and Marcel Thaens presents the paper on public administration science and practice, the debate on e government concentrates on service delivery, information and technology. This article argues that we need a broad public administration approach towards e-government that surpasses this technocratic emphasis. Public administration theory helps us to escape from the conceptual prison of the information management ideology that currently dominates e-government. Both the locus of e-government (the parts of public administration that are being touched by it) and its focus (its approach towards governance) can be used to broaden the concept. If we do not enrich egovernment, many of its possibilities will remain unexploited. Also, if we stick to the information management approach, e-government will endanger the very foundations of the legitimacy of public administration.[1]

Jensen J. Zhao, Sherry Y. Zhao provide a study assessed the security of the U.S. state e-government sites to identify opportunities for and threats to the sites and their users. The study used a combination of three methods – web content analysis, information security auditing, and computer network security mapping – for data collection and analysis. The findings indicate that most state e-government sites posted privacy and security policy statements; however, only less than half stated clearly what security measures were in action. Second, the information security audit revealed that the sites secured users' accounts with SSL encryption for data transmission, and the sites' search tools enable public users to search for public information only. Third, although the sites had most of their internet ports filtered or behind firewalls, all of them had their main IP addresses detected and their port 80/tcp open. The study discussed the threats and opportunities and suggested possible solutions for improving e-government security.[2]

Andrea Ko and Balint Molnar gives an overview about the most frequently cited identity management architectures (namely: Liberty Alliance Architecture, Sibboleth, Government GatewayModel and Austrian Model) and presents an identity management framework (based on the PKI, but improved it), customized for the Hungarian specialities, which offer possibilities to improve the related services quality.[3]

In this section, we briefly review the related work on Block chain technology.

R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens present the concept between two arrangements of electric vehicles, which fundamentally diminish the effect of the charging procedure on the power framework amid business hours. This trading approach is also economically beneficial for all the users involved in the trading process. An activity-based approach is used to predict the daily agenda and trips of a synthetic population for Flanders (Belgium) [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han provide a study of the possible flow and functional factors that enable DET in communication networks. Various design issues on how to implement DET in practice are discussed. An ideal approach is created for delay-tolerant remote controlled correspondence organizes in which every remote powered device can masterminded its information transmission and energy exchanging activities as indicated by present and future vitality accessibility [2].

III. PROPOSED SYSTEM:

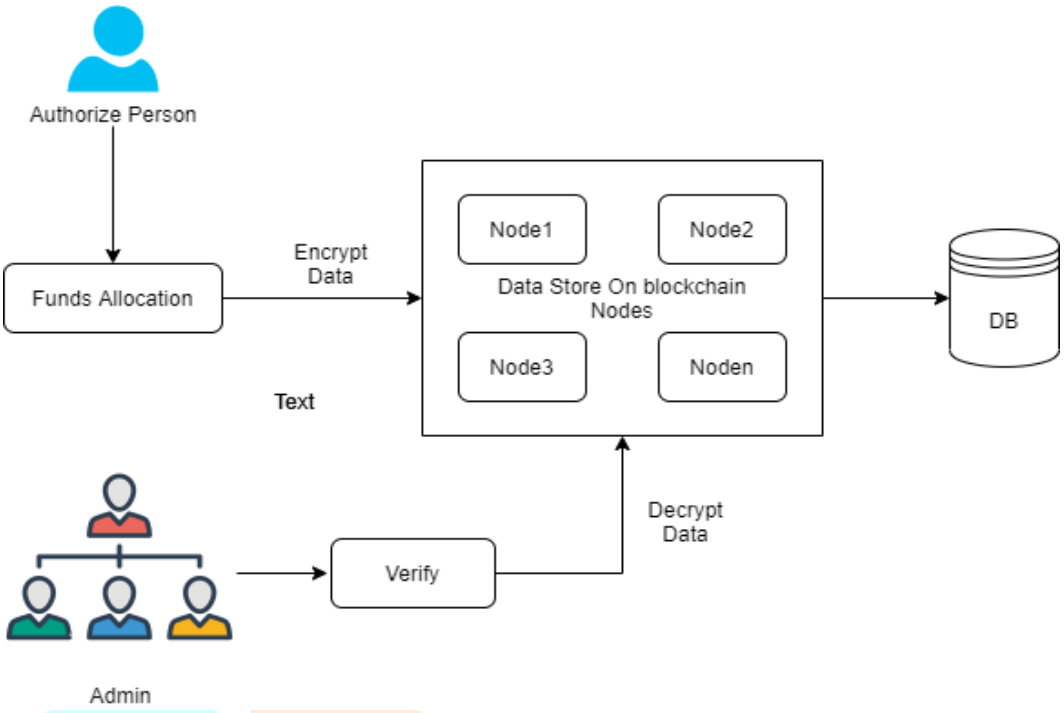

Figure 1. System Architecture

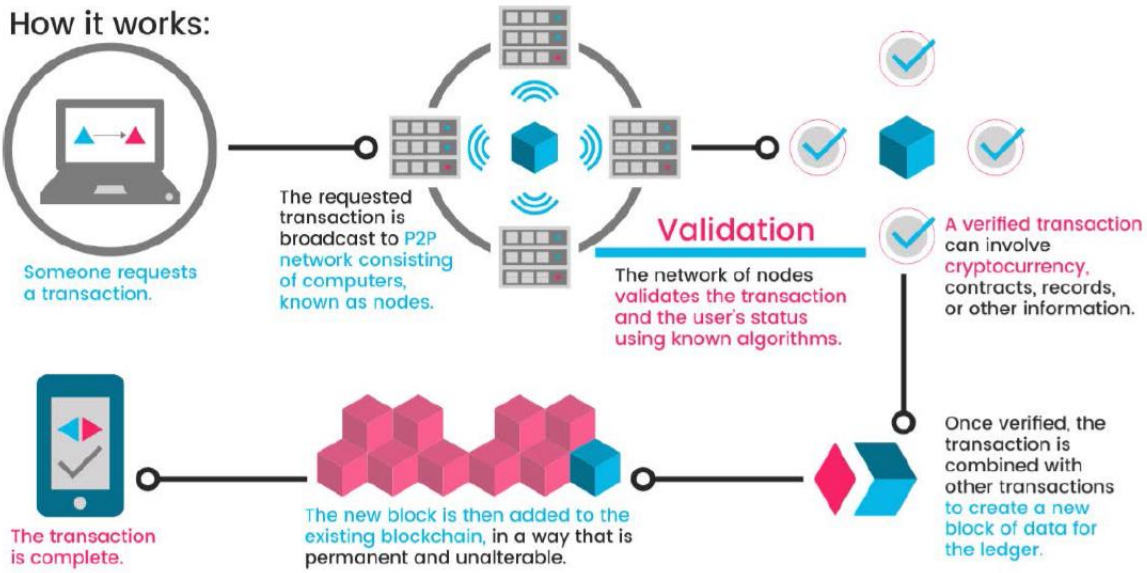

Figure 2. Blockchain

IV. MODULES:

1. Module 1 - Government: - Government will give the fund which is requested by the user.
2. Module 2 – Admin Team:- This will authorize or verify the user that it is a valid user as well as valid request or not.
3. Module 3 - Customer:- User will request for the fund according to their needs.

V. IMPLEMENTATION :

To achieve our goal of developing a decentralized Government funding system, we have designed and implemented a robust platform that leverages smart contracts to securely and transparently store and verify users' data transactions. Our system has undergone extensive evaluation, taking into consideration key factors such as security, ease of use, and decentralization.

At the core of our decentralized government funding system, we have created several classes to effectively manage and store users' identity, name, location, and other relevant information. These classes serve as the foundation for maintaining a reliable and organized user database within the system.

By utilizing cryptographic hashing, we can verify the integrity of the transaction at any point in the future, providing assurance that no tampering has occurred.

In order to implement a government fund allocation system using blockchain, several technical steps were undertaken. Firstly, the system requirements were defined, which included identifying the government entities involved, specifying the types of funds to be allocated, and determining transparency and security requirements. Smart contracts were designed to govern the fund allocation process, including contracts for fund request, approval, disbursement, and auditing. These contracts incorporated the necessary data structures and functions to enforce fund allocation rules and ensure transparency.

Extensive testing was conducted to validate the functionality and security of the smart contracts. A user-friendly frontend interface was developed to allow government officials, fund recipients, and auditors to interact with the system. This frontend was integrated with the blockchain backend using appropriate APIs. The blockchain network was set up, either on a private or public network, and the smart contracts were deployed. Thorough testing was performed to ensure the system's performance, scalability, and security. The implemented system provided enhanced transparency, accountability, and efficiency in the government fund allocation process.

The proposed system aims to track the journey of funds allocated to the government at each stage of the government process. To achieve this, the researcher proposes the utilization of key pair generation algorithms to establish secure communication channels between relevant entities involved in the fund allocation process. Key pairs, consisting of public and private keys, can provide secure and authenticated transactions within the blockchain network. The use of metadata file decryption algorithms to ensure that encrypted metadata associated with fund allocation transactions can be decrypted securely by authorized entities. This process allows for the verification of transaction details and improves the transparency of the fund allocation process.

A smart contract is a self-executing digital contract with the terms of the agreement written directly into code on a blockchain. It automatically enforces the terms, verifies transactions, and facilitates interactions between parties without the need for intermediaries. Smart contracts provide transparency, security, and efficiency in various decentralized applications and eliminate the need for trust in traditional contract enforcement.

Smart contracts are used in blockchain-based voting systems for several reasons:

Transparency: Smart contracts provide transparency in this process. The code of the smart contract is visible to all participants, ensuring that the rules and procedures are clear and cannot be altered without consensus.

Security: Smart contracts utilize cryptographic techniques to secure the voting process. The immutability of the blockchain ensures that once a vote is recorded, it cannot be altered or tampered with.

Decentralization: Blockchain-based systems leverage the decentralized nature of the technology. Smart contracts are executed on a network of nodes, eliminating the need for a centralized authority or trusted intermediaries. This decentralized approach ensures that no single entity has control over the process, making it more resistant to censorship and manipulation.

Our decentralized system combines smart contracts, advanced encryption techniques, and secure validation processes to create a secure and transparent platform.

It focuses on enhancing the security of the government fund allocation process using blockchain algorithms. Specifically, the Advanced Encryption Standard (AES) algorithm is employed for encryption and decryption. AES is a widely recognized and robust encryption method that ensures the confidentiality and integrity of sensitive data.

VI. ALGORITHM:

1. AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used 128-bit block with 128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round: 10, 12, 14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

Cipher text (128 bit)

2. MD5(Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Steps:

a) A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
b) The output of a message digest is considered as a digital signature of the input data.
c) MD5 is a message digest algorithm producing 128 bits of data.
d) It uses constants derived to trigonometric Sine function.
e) It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
f) Most modern programming languages provides MD5 algorithm as built-in functions

VII. RESULTS AND DISCUSSION:

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i3-2120 CPU @ 3.30GHz, 4GB memory, Windows 7, MySQL 5.1 backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.

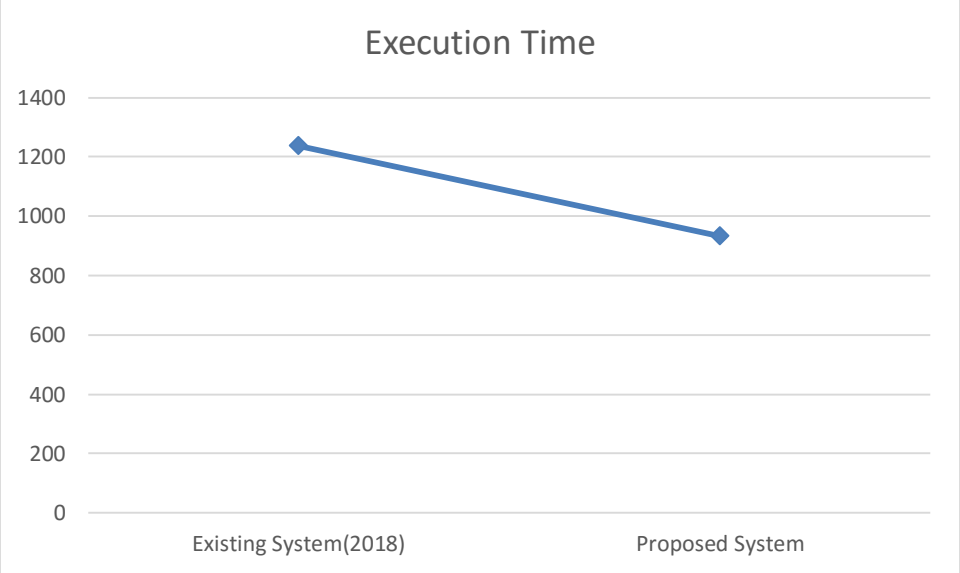

Figure 5: overall system execution graph

Existing System	Proposed System
1236	932

Table6: overall system execution table

VIII. CONCLUSION:

In this project, we have to consider about the blockchain applications, we even have to consider the access and privacy challenges though. This allows to maintain crystal clear record with on demand right to transactional data on a need to know basis. The system makes use of encryption to secure transactional data using hashes to maintain a block of transactions in a chain manner which is maintained and verified by every node involved to verify the transaction and save the data in a transparent form within the government. The system allows for a full proof, secure and authentic fund allocation and fund tracking system to help form an incorruptible government process. Even then, with further enhancements, this blockchain model can provide a transparency in all the government transactions. There will be no discrepancies of any kind. Because of the decentralized ledger all the transactions can be verified and cannot be altered. The money that is released can be tracked, anyone and everyone can find out how the money is being used. Such a blockchain will surely reduce the ongoing corruption It will create a huge impact on the economic development of a country.

IX. ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on 'Government Fund Allocation Using Blockchain '. We would like to take this opportunity to thank our internal guide Prof. Hema Kumbhar for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. Vina Lomte, Head of Computer Engineering Department, RMDSSOE for her indispensable support, suggestions.

We are also immensely grateful to Prof. Sonal Fatangare for sharing their pearls of wisdom with us during the course of this research, and we thank them for their insights, although any errors are our own and should not tarnish the reputations of these esteemed persons.

In the end our special thanks to Dr.V.V. Dixit, Principal, RMDSSOE for providing various resources such as laboratory with all needed software platforms, continuous internet connection, for our Project.

REFERENCES:

[1] [1 R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," IEEE Intell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

[2] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[4] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Comput.

[5] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.

[6] S. Barber et al, "Bitter to better-how to make bitcoin a better currency," in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.

[7] I. Alqassem et al., "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in Proc. IEEE Internet Things, IEEE Int. Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.

[8] K. Croman et al., "On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.

[9] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[10] L. Luu et al., "A secure sharding protocol for open blockchains," Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.