iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52226

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Survey on Government Fund Allocation Using Blockchain

Jay Jagtap[1], Pradhumna Jadhav[2], Rushikesh Wanjale[3], Ninad Mane[4], Mrs. Hema Kumbhar[5]
[1, 2, 3, 4]*U.G. Student, Department of Computer Engineering, RMD Sinhgad School of Engineering, Maharashtra, India*
[5]*Project Guide, Department of Computer Engineer, RMD Sinhgad School of Engineering, Maharashtra, India*

Abstract: ***Governments have a lot of responsibilities, which involves a lot of money transactions for various projects, employees, and farmer schemes. Corruption is a big problem as it's hard to track and can slow progress. We can solve this by using blockchain technology.***
Blockchain is a list of records that are linked and secured using cryptography. Each record contains transaction data, a timestamp, and a cryptographic hash of the previous record. We use security algorithms like AES encryption and decryption to protect the data.
This project proposes a system to track government funds using key pair generation, metadata file decryption, and data verification algorithms.
This will ensure transparency and accountability at every stage of the transaction. Blockchain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. In this project researcher use Blockchain Algorithms for security like AES for Encryption and Decryption By design, a blockchain is resistant to modification of the data. In this project we propose a system to track funds allocated to the government as they travel through the government process at each stage using Key pair generation algorithm, Metadata file decryption and Data verification algorithms.
Keywords: Blockchain, HyperLedger, Security, Transparency, Encryption, Government Funds, Cryptography, AES.

I. INTRODUCTION

India, widely regarded as the world's fastest-growing economy, holds immense potential for attracting international customers and leveraging cutting-edge technologies to drive growth and development. Digitalization, in particular, presents numerous opportunities to enhance connectivity and transform various sectors of the economy. However, the adoption and distribution of these technologies remain uneven across some government sectors. To achieve optimal value and efficiency, it is crucial to keep pace with emerging technologies, such as blockchain, which is increasingly being used across diverse industries worldwide. Its decentralized, secure, unchangeable, and tamper-proof nature makes it an ideal solution for addressing the lack of transparency and accountability in the management of public funds in India. By leveraging blockchain technology, it is possible to create a highly secure and immutable environment for tracking and managing public funds, ensuring optimal utilization and accountability.

II. RELATED WORK

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 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].

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a work to accomplishes request reaction by giving motivating forces to releasing PHEVs to adjust nearby power request out of their own selfinterests. Be that as it may, since exchange security and security insurance issues show genuine difficulties, they investigate a promising consortium block-chain innovation to enhance exchange security without dependence on a confided in outsider. A restricted P2P Electricity Trading framework with Consortium block- chain (PETCON) strategy is proposed to represent detailed activities of limited P2P power exchanging [3].

N. Z. Aitzhan and D. Svetinovic presents a work that address the issue of providing transaction security in decentralized smart grid energy trading without confidence on trusted third parties. We have developed a proof-of-concept for decentralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging flows, enabling peers to anonymously negotiate energy prices and securely perform trading transactions [4].

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now presents a work that shows decentralized computerized cash, called NRG-coin. Prosumers in the smart grid framework exchange privately made sustainable power source utilizing NRG-coins, the estimation of which is indented on an open cash trade advertise. Like Bit-coins, this money proposes various favorable circumstances over fiat cash, however not at all like Bit-coins it is made by infusing vitality into the matrix, as opposed to giving vitality on computational influence. Likewise, they make a novel exchanging worldview for purchasing and offering environmentally friendly power vitality in the smart grid network [5].

S. Barber et al presents a work that Bitcoin is isolated computerized cash which has pulled in a significant number of clients. They play out a top to bottom examination to comprehend what made Bit-coin so effective, while many years of research on cryptographic e-money have not prompt a vast scale appropriation. They ask additionally how Bit-coin could turn into a decent contender for seemingly perpetual stable money [6].

I. Alqassem et al presents a work that Bitcoin is constantly improved by an open source network, and different Bit-coin libraries, APIs, and elective usage are being created. All things considered, there is no up and coming convention contrast or design portrayal since the authority whitepaper was distributed. The work demonstrates an a la mode convention detail and design investigation of the Bit-coin framework. We play out this examination as the initial move towards determination of the cryptographic currency reference design [7].

K. Croman et al presents a work that the expanding fame of block-chain-based digital forms of money has made versatility an essential and earnest obligation. The work ponders how essential and incidental bottlenecks in Bit-coin restrict the ability of its present distributed overlay system to help generously higher throughputs and lower latencies. These outcomes propose that re-parameterization of square size and interruption ought to be seen just as a first augmentation toward accomplishing people to come, high-stack block-chain conventions, and real advances will moreover require a fundamental re-evaluating of specialized ways [8].

G. W. Peters and E. Panayi presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements [9].

L. Luu et al presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO scales exchange rates straight with accessible estimation for mining: the more the calculation control in the system, the higher the quantity of exchange squares chosen per unit time. ELASTICO is productive in its system messages and permit complex foes of up to one-fourth of the aggregate computational power [10].

III.EXISTING APPROACH

Numerous approaches have been implemented in the field of government funding to enhance the security, reliability, and efficiency of the funding process. These efforts are distinct from the algorithms used in government fund allocation systems. Despite these advancements, the existing system still have security risks that can compromise the integrity of the process. Human error and technical malfunctions can occur, while it is vulnerable to hacking, political Influence, system failure, and other threats from both domestic and foreign saboteurs. To address these issues, researchers and experts in this field continue to develop and implement innovative solutions. These include the use of blockchain technology to enhance security, the development of cryptographic protocols to protect privacy, and the use of advanced statistical techniques to ensure accurate vote counting. Overall, the ongoing efforts to enhance government fund allocation systems are critical to ensuring the reliability and trustworthiness of the funding process.

IV. PROPOSED APPROACH

The Smart E-voting system we developed uses blockchain concepts and a web interface to provide a secure online voting experience. To ensure security, voters are required to confirm their identity with a high-security OTP and their Aadhar Card before their vote is added to the main database. Another feature of the system is that voters can confirm that their vote has been counted for the correct candidate or party. The system automatically tallies the votes, which saves a lot of time, and enables the Election Commissioner of India to announce the results quickly. Overall, our proposed Smart E-voting system provides a secure, user-friendly, and efficient way for voters to participate in the democratic process.

A. Flow Diagram

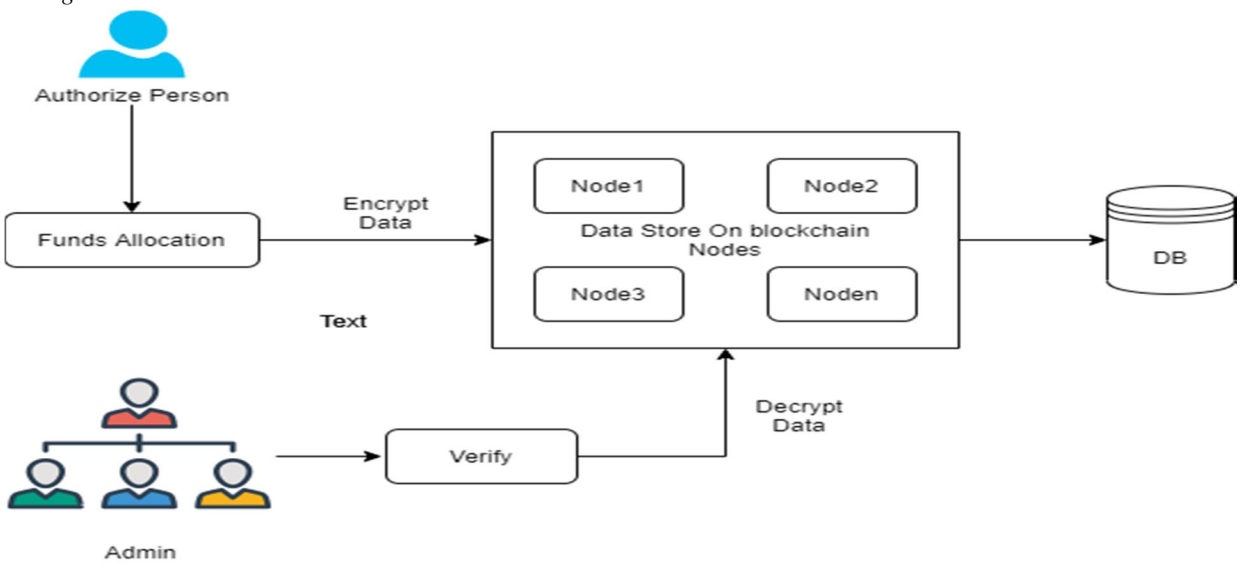


Fig.1 : Block diagram of government fund allocation system

B. Algorithm

AES Algorithm for Encryption.

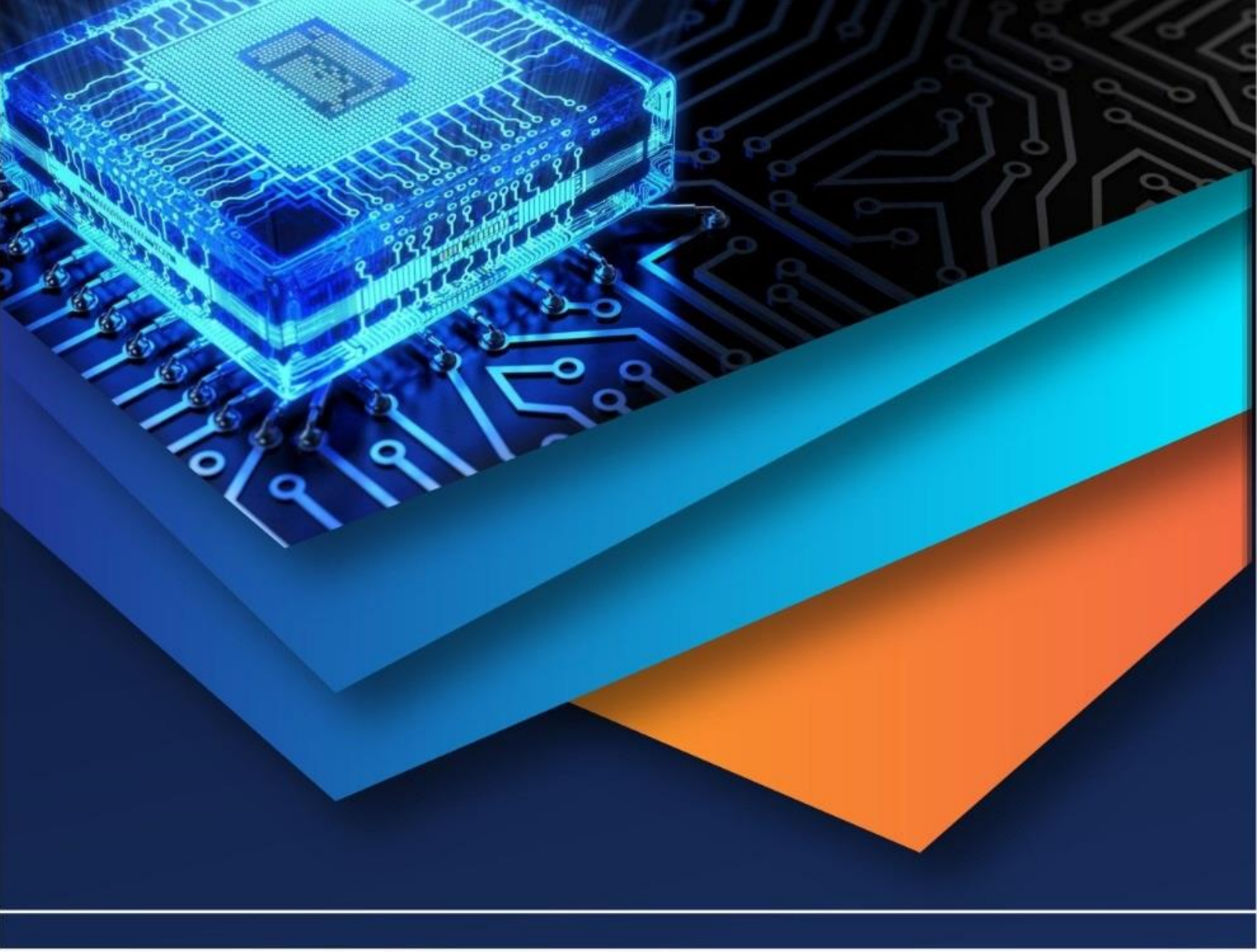
The AES (Advanced Encryption Standard) algorithm is a symmetric algorithm used to convert plain text into cipher text for secure transmission or storage. It was developed to address the weaknesses of the DES (Data Encryption Standard) algorithm, which had a 56-bit key and 64-bit block size that were no longer secure against modern attacks. The AES algorithm uses a block size of 128 bits and keys of 128, 192, or 256 bits. It was developed by Joan Daemen and Vincent Rijmen, who called it Rijndael. To encrypt data using AES, the algorithm takes in a secret key and plain text input of the same bit size (e.g., 128-bit key and 128-bit input). The algorithm then processes the input through 10, 12, or 14 rounds, depending on the key and input size. Each round consists of four steps: substitution of the input bytes, shifting of the rows, mixing of the columns, and adding of the round key. The final round differs slightly from the previous rounds. The output of the AES algorithm is the cipher text, which is the encrypted version of the plain text input. The cipher text is also of the same size as the input, typically 128 bits for most modern applications.

V. CONCLUSION

This paper described, 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.

REFERENCES

[1] Sahil Siddharth Jambhulkar, Vishakha Prashant Ratnaparkhi (2020) "Government Fund Distribution and Tracking System Using Blockchain Technology", International Journal of Emerging Technologies and Innovative Research, ISSN:2349-5162, Vol.7, Issue 9, page no.1379-1387..
[2] Abhishek Katore, Sanskar Choubey, (2021) "Government Scheme and Funds Tracker using Blockchain", International Journal of Engineering Research and Technology (IJERT), Volume 10, Issue 05.
[3] P. Joshi, S. Kumar, D. Kumar, and A. K. Singh, (2019) "A BlockchainBased Framework for Fraud Detection", Conference on Next Generation Computing Applications (Next Comp).
[4] Meghna Vadher Shivani Pandey, Darshana Sawant, Hezal Lopes (2021) "State Government Fund Allocation and Tracking System using Blockchain Technology", International Journal of Emerging Technologies and Innovative Research ISSN:2349-5162, Vol.8, Issue 6, page no. a455-a459..
[5] A. Chauhan, G. Savner, P. Venkatesh, V. Patil and W. Wu, (2020) "A Blockchain-Based Tracking System", IEEE International Conference on Service Oriented System Engineering (SOSE), Oxford, United Kingdom.
[6] S. Barber et al, "Bitter to betterhow 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.
[11] 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.
[12] Mark G, Melinda N, Lisa P, George Bell, Jonathan Downing, Kaivan Rahbari, Moh Kilani, Katlyn Woods, Scott S, Curtis T,Everette J, Aaron Varrone, "BLOCKCHAIN AND SUITABILITY FOR GOVERNMENT APPLICATIONS", 2018 Public-Private Analytical Exchange Program.
[13] Dave Bryson Dave Penny David C. Goldenberg Gloria Serrao, "BLOCKCHAIN TECHNOLOGY FOR GOVERNMENT", MITRE December 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY