International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228340

Government Fund Disbursement Using Blockchain

Kshitija Chaudhari[1], Indrajeet Badhe[1], Omkar Rasane[1], Santosh Bendre[1], Prof. Shakil B. Tamboli[2]

[1]Student, Department of Computer Engineering, Zeal College of Engineering and Research, Pune Maharashtra India

[2]Professor & Guide, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

Article Info
Volume 8, Issue 3
Page Number : 518-523

Publication Issue :
May-June-2022

Article History
Accepted: 10 May 2022
Published: 30 May 2022

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 drawback 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, 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, Hyper Ledger, Security, Transparency, Encryption, Government Funds, Cryptography, AES.

I. INTRODUCTION

A. 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.

B. Motivation

- Now a days 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.

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 self-interests. 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 Bit-coin 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 Bit-coin 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

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 reevaluating 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].

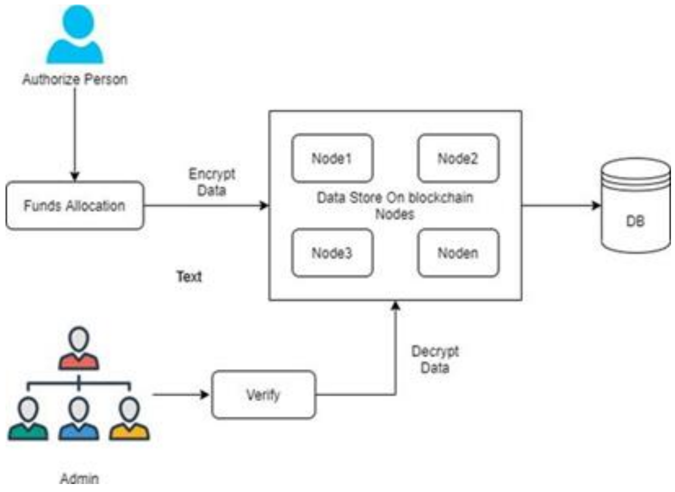
L. Luu et al presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO scales exchange rates straightly with accessible estimation for mining: the more the calculation control in the system, the higher the quantity of exchange 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. PROPOSED SYSTEM

Modules:

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

currency reference design [7].



IV. ALGORITHM

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 algo 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 asweak. AES was to be used128-bitblock with128-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 inputXor state block (i/p)

Final round:10,12,14

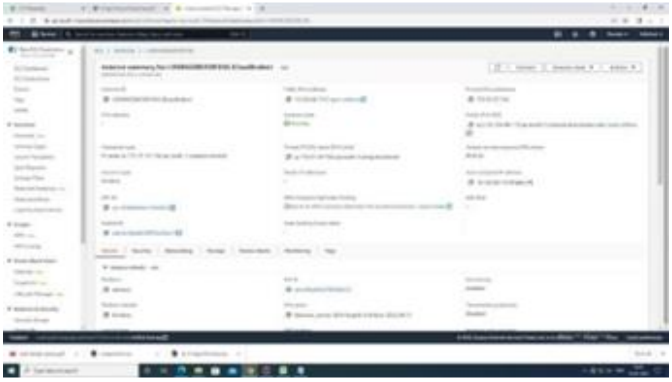
Each round consists: sub byte, shift byte, mix columns, add round key.

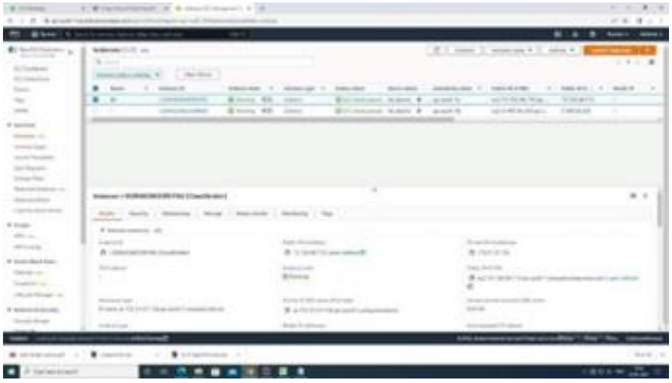
Output:

cipher text (128 bit)

V. RESULT AND DISCUSSION

Goverment Scheme
PRADHAN MANTRI JAN DHAN YOJNA
PMJDY Scheme- Open Zero Balance Account
Pradhan Mantri Awas Yojana





VI. 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 totransactional data on a need to know basis. The system makes use ofencryption to secure transactional data using hashes to maintain a block oftransactions in a chain manner which is maintained and verified by every nodeinvolved 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.

VII. REFERENCES

[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.