



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.512

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com



Government Fund Distribution and Tracking System

Shivani Kadam, Mridul Saini, Pralay Patil, Vaishnavi Kad, Prof. ME. Sanap

Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, Maharashtra, India

ABSTRACT: A block chain is a developing listing of records, known as blocks that are related using cryptography. Every block carries a cryptography hash of the previous block, a timestamp, and transaction data. By design, a Blockchain is resistant to modification of the data. In this we propose a system to track funds allocated to the government as they travel through the government process at each stage. This system makes use of block chain generation to preserve the transparency and protection at each degree as the fund flow ahead. This machine permits to maintain the crystal clean record with all customers who are linked inside the chain to transaction the records on a need to recognize foundation. The system makes use of encryption to secure transactional statistics using hash values to keep a block of transactions in a sequence way which is maintained and confirmed by each node concerned to affirm the Transaction and keep the facts in obvious form within the authorities. The application permits for a complete proof, comfortable and true fund allocation and fund tracking application help to form an incorruptible government process.

KEYWORDS: Blockchain, security, transparency, encryption, government funds, cryptography.

I. INTRODUCTION

Blockchain is touted for its capability to enhance the trust and transparency of data primary based transactions among individuals and organizations. The technology offers promise while strategically implemented in the proper contexts. However what are the conditions below which block chain makes experience and how would possibly the generation be beneficial while carried out in authorities? Historically, organizations running their very own, man or woman IT systems looking for to collaborate should reckon with challenges which include reconciliation of facts, figuring out a single source of fact, and facilitating duty. Blockchain generation addresses those demanding situations via presenting a technical foundation that supports the execution of shared commercial enterprise approaches in a way that no unmarried entity controls the entire machine. Government has an inherent want to build, preserve, and protect public accept as true with in statistics and structures.

In some situations, blockchain may additionally help decorate this trust. Traditional relational database control solutions (e.g. Oracle and square), deployed globally across thousands and thousands of packages, have one predominant operational constraint the control of facts is finished by a few entities who must be trusted. Distributed Ledger technologies (DLT, typically called blockchain), an alternative architectural approach to coping with facts, and gets rid of the want for a relied on authority to store and proportion a continually growing set of facts. Blockchain have digital signatures and use keys to authorize and take a look at transactions and definitely discover the initiator. Once recorded to the chain, a blockchain record cannot be deleted or manipulated. New blocks might also most effective be appended to the chain, making sure facts integrity and growing a verifiable audit path? Because the name connotes, blockchain is a series of blocks. Each block represents a report or set of information, this is connected to others with cryptography. Every block consists of a few available statistics to provide public expertise about the movement, time, or some other feature of the report, developing a public transcript of the way the records develops, called a "ledger." A transaction enters a blockchain gadget, a consensus version is hired to determine which subsequent set of valid transactions, or block, have to be appended to the ledger. Due to the fact consensus is mounted over a distributed network for nodes, there's no imperative authority that governs the validation and inclusion of new transaction facts. As maximum blockchain software program is open source, the guidelines that adjudicate the blocks and blanketed transaction statistics are available for assessment. For public blockchain structures, the statistics itself is available for direct commentary through everybody who cares to get entry to it. This makes open blockchain datasets perceived as more reliable to an extra number of customers.



II. MOTIVATION

Usually when a project is allocated funds, there is no knowledge as to how these funds are being used and a large part of it is never shown in records due to corruption. To solve this problem, a system has been proposed using Blockchain to provide the transparency.

- A major hurdle that the top government faces is the low-level corruption that is sometimes impossible to track which deprives the state progress.
- Blockchain technology is an upcoming technology and said to be one of the most promising technologies which would revolutionize the world.

III. 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.

This paper provides, through its methodology, a detailed analysis of the block-chain fit in the supply chain industry. It defines the specific elements of block-chain that affect supply chain such as scalability, performance, consensus mechanism, privacy considerations, location proof & cost.[2]

Data mining framework for avoidance & revealing of financial statement fraud in this study. The framework used in this research follows the conventional flow of data mining. These useful variables are being used for implementing association rule mining for prevention and three predictive mining techniques namely K-means, Multi-Level Feed Forward Network, Genetic programming for detection of financial fraud.[4]

In this paper, the author proposes a block-chain enable well-organized data collection and secure sharing scheme combining Ethereum block-chain and deep reinforcement-learning (DRL) to create a reliable and safe environment. In this scheme, DRL is used to attain the highest amount of collected data, & the block-chain technology is used to guarantee safety & reliability of data sharing. [5]

This paper proposed a new information sharing scheme based on blockchain technology. Users can manage their data and understand the data being collected about them and how to use it without trusting any third party. However, the scheme did not take into account the possibility of the enterprise itself tampering with data. [10]

The author presented, product traceability gadget primarily based on blockchain era, wherein all product transferring histories are forever recorded in an allotted ledger by means of the usage of clever contracts and a chain is shaped which could hint back to the source of the products. [9]

IV. PROBLEM STATEMENT

Governments want to cater to a massive range of duties of a state. The working of state governments includes large variety of transactions in the direction of numerous operations that want to be finished all through the state. This includes new tasks, restore and preservation works, awarding contracts, paying of government employees, farmer schemes and so on. A main impediment that the top government faces is the low level corruption that is occasionally now not feasible to tune which deprives the nation development. Tracking it is a very complicated task due to the current application.

V. PROPOSED METHOD

The proposed system is used to track the funds allocated to the state government as they travel through the government process at every stage. We here make use of blockchain technology to secure the transactions at every level while preserving transparency in each transaction sealing each transaction with proofs because the price range circulate ahead. This let sin retaining crystal clear report with on demand proper to transactional facts on a need to realize basis. The system makes use of encryption to comfortable transactional facts by hashes to preserve a block of transactions in a sequence way that is maintained and tested via each node concerned to authenticate the transaction & keep the facts



in a transparent shape within the authorities. The system lets in for full evidence, cozy & real fund allocation and fund monitoring system to help form an incorruptible government procedure.

In this we are using 3 modules i.e. User and Government and Authority.

Module 1 - Government:- Government will give the fund which is requested by the user.

Module 2 – Authority:- This will authorize or verify the user that it is a valid user as well as valid request or not.

Module 3 - User (Customer):- User will request for the fund according to their needs.

Architecture

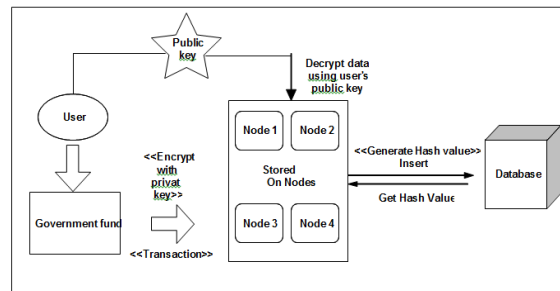


Fig.2 System Architecture

VI. METHODOLOGIES

1. Encryption

Data encryption interprets records into some other form, or code, in order that most effective people with get admission to a Secret (unique) key (formally known as a decryption key) or password can examine it. Encrypted information is commonly referred to as cipher-textual content, while unencrypted data is referred to as plaintext.

2. Decryption

The conversion of encrypted information into its original shape is known as Decryption. It's far typically a reverse technique of encryption. It decodes the encrypted information so that a certified consumer can only decrypt the records because decryption calls for a secret key or password.

3. Hashing Concept

A hash cost is a numeric cost of a set period that uniquely identifies information. Hash values represent large quantities of data as whole lot smaller numeric values, so they're used with virtual signatures. You may signal a hash price more correctly than signing the larger price. Key generation

4. Advanced Encryption Standard

The more popular and widely followed symmetric encryption algorithm in all likelihood to be encountered in recent times is the advanced Encryption well known (AES). It's far located at the least six times faster than triple DES.

An alternative for DES was needed as its key length changed into too small. With growing computing energy, it changed into taken into consideration inclined in opposition to exhaustive key search attack. Triple DES turned into designed to overcome this drawback however it changed into located slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java



Operation of AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

5. Secure Hashing Algorithm (SHA)

The maximum adopted relaxed algorithms related to the blockchain era are (SHA-1, SHA2, and SHA-256) encryption due to their particular best of hash characteristic that create precise outputs when given special inputs [31,32]. The hash characteristic right here is a unique key created to discover transaction that on the same time identifies an man or woman. This set of rules is efficient in verifying record and message integrity during transaction, statistics identification, and password verification.

Hashing Functions

Hashing functions take some data as input and produce an output (called hash digest) of fixed length for that input data. This output should, however, satisfy some conditions to be useful.

- **Uniform distribution:** Since the length of the output hash digest is of a fixed length and the input size may vary, it is apparent that there are going to be some output values that can be obtained for different input values. Even though this is the case, the hash function should be such that for any input value, each possible output value should be equally likely. That is to say that every possible output has the same likelihood to be produced for any given input value.
- **Fixed Length:** This should be quite self-explanatory. The output values should all be of a fixed length. So, for example, a hashing function could have an output size of 20 characters or 12 characters, etc. SHA-512 has an output size of 512 bits.
- **Collision resistance:** Simply speaking, this means that there aren't any or rather it is not feasible to find two distinct inputs to the hash function that result in the same output (hash digest).

Hashing Algorithm — SHA-512

SHA-512 does its work in a few stages.

1. Input formatting
2. Hash buffer initialization
3. Message Processing
4. Output

VII. CONCLUSION

In this paper, we considered about the blockchain applications, we even have to consider the access and privacy challenges though. 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. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory”, IEEE Transactions on Industrial Informatics Volume: 15 , June 2019.
2. Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, “Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment”, MDPI January 2019.



3. Mrs. R.Meenatkshi , Mrs. K.Sivaranjani, “A Comparative Study on Fraud Detection in Financial Statement using Data Mining Technique”, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.7, July-2016, pg. 382-386.
4. Analysis KK Tangod, GH Kulkarni, “Detection of Financial Statement Fraud using Data Mining Technique and Performance”,International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015 .
5. Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. “Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning”, IEEE Transaction on Industrial Volume: 15, Issue: 6 , June 2019
6. Apoorva Mohite, Ajay Acharya, “Blockchain for government fund tracking usingHyperledger”, IEEE Transactions on Fuzzy Systems, April 2018.
7. Ning Wang, Jing-Chao Sun, Meng JooEr,“Tracking-Error-Based Universal Adaptive FuzzyControl for Output Tracking of Nonlinear Systemwith Completely Unknown Dynamics” ,IEEEAPRIL 2017.
8. Adam Ghandar, Zbigniew Michalewicz, Ralf Zurbruegg, Chee Cheong,“Index Tracking Fund Enhancement Using Evolving Multi-CriteriaFuzzy Decision Models”,IEEE Congress on Evolutionary Computation.
9. Shangping Wang, Dongyi Li, Yaling Zhang, Juanjuan Chen, “Smart Contract-Based Product Traceability System in the Supply Chain Scenario”, IEEE Access, 2019.
10. M. Nakasumi, “Information Sharing for Supply Chain Management Based on Block Chain Technology,” in 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece, Jul. 2017.
11. M. Kim, B. Hilton, Z. Burks, and J. Reyes, “Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution,” in 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Univ British Columbia, Vancouver, Canada, Nov. 2018.
12. Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, “A Hybrid Blockchain Ledger for Supply Chain Visibility,” in 2018 17th International Symposium on Parallel and Distributed Computing (ISPDC), Geneva, Switzerland, Aug. 2018.
13. T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere - a use-case of blockchains in the pharma supply-chain,” in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, Jul. 2017.
14. X. Ye, Q. Shao, and R. Xiao, “A supply chain prototype system based on blockchain, smart contract and Internet of Things,” Science & Technology Review, vol. 35, no. 23, pp. 62–69, 2017.
15. Q. Lu and X. Xu, “Adaptable Blockchain-Based Systems: A Case Study for Product Traceability,” IEEE Softw., vol. 34, no. 6, pp. 21–27, Dec. 2017.



INNO  **SPACE**
SJIF Scientific Journal Impact Factor

**Impact Factor:
7.512**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details