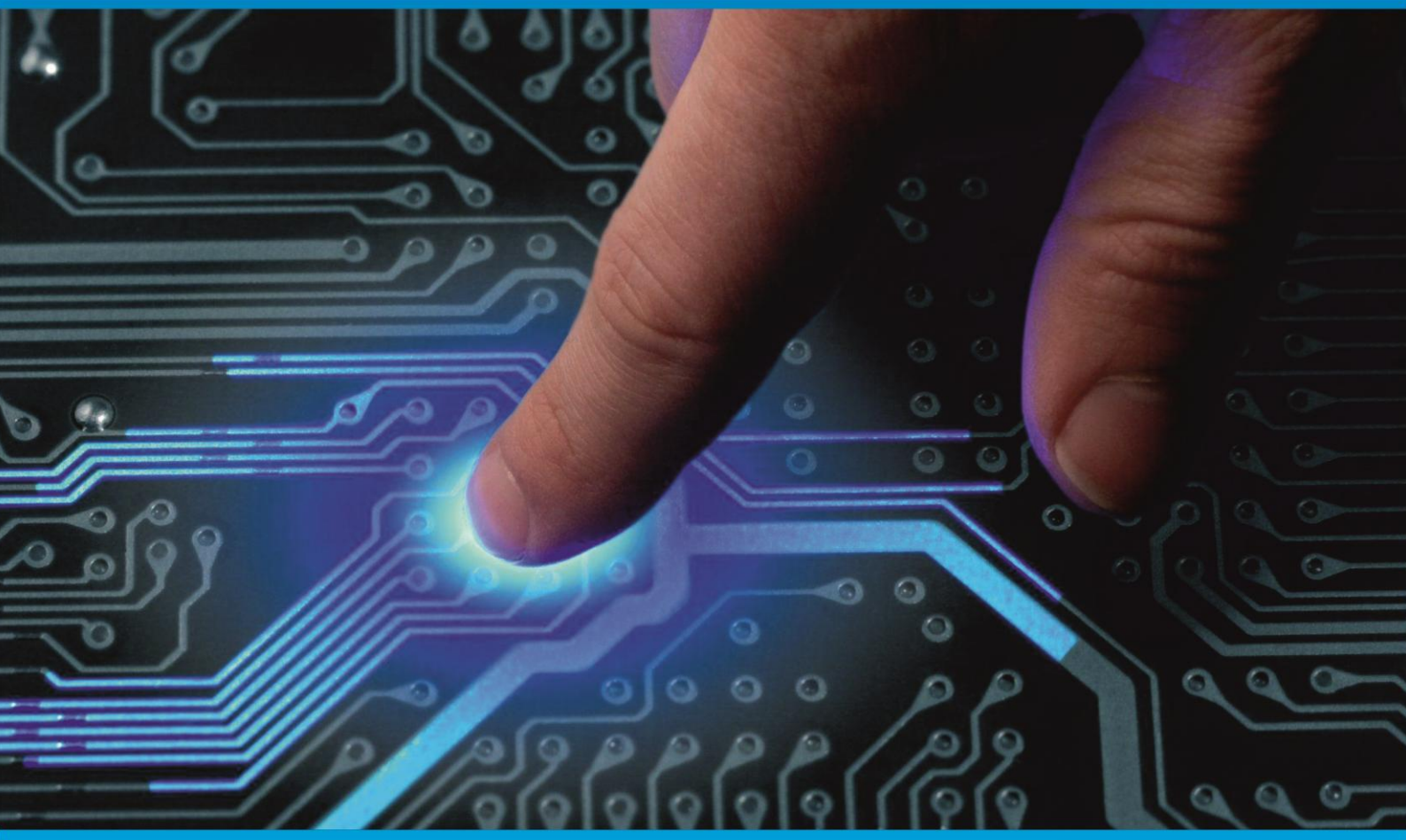
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

Government Fund Distribution and Tracking System

Shivani Kadam[1], Mridul Saini[2], Pralay Patil[3], Vaishnavi Kad[4], Prof. M.E. Sanap[5]

BE Students, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[1,2,3,4]

Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[5]

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 agree with and transparency of dataprimarilybased transactions among individuals and organizations.The technology offers promise whilst strategically implemented inthe proper contexts. however whatarethe conditions below whichblockchainmakes experience andhow woul dpossibly the generation be beneficial whilst carriedout in authorities? historically, organizations running their veryown, ma norwoman IT systems lookingfor tocollaborate should reckonwith challenges whichinclude reconciliationof facts, figuringo ut a single source of fact,andfacilitating duty.Blockchaingeneration addresses those demandingsituations via presenting atec hnical foundation that supports theexecutionofshared commercialenterprise approaches ina way thatno unmarried entitycont rolsthe entire machine. government hasaninherent want to build, preserve,and protect public acceptastruewith in statistics a nd structures.

In some situations,blockchain mayadditionally help decorate this trust. traditional relational database control solutions (e.g. Oracle and square), deployed globally across thousands and thousands of packages,haveone predominant operationalconstraintthe control of facts is finished by afew entitieswhomustb etrusted.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 thers with cryptography, every block consistsof afew 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 transactions enter a blockchain gadget, a consensus version is hired to determine which subsequent setof valid transactions,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

or block, have to be appended to the ledger. due to the fact consensus is mounted overa distributed network for nodes, there's no imperative authoritythatgovernsthevalidationandinclusion ofnew transaction facts.As maximum blockchai n softwareprogram isopen source,the guidelines thatadjudicatetheblocksand blanketed transaction statistics are available for assessment.Forpublicblockchain structures,the statistics itselfis available for direct commentary through everybody who cares to getentry to it.Thismakesopenblockchaindatasetsperceivedofas more reliable toa extra number of customers.

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 show 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.

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.

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 follow 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 propose 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 a 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]

III.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,

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

paying of government employees, farmer schemes and so on. A main impediment that the top government face 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.

IV.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 thetransactionsat every level while preserving transparencyin each transactionsealing ea ch transactionwithproofs becausethe pricerange circulate ahead.This letsin retaining crystal clear report withondemand pro per totransactional 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 thatis maintainedand tested via each node concerned to authenticate the transaction & keep the facts In a transparent shape withinthe authorities.The system letsin fora full evidence, cozy & real fundallocationandfund monitorin g 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

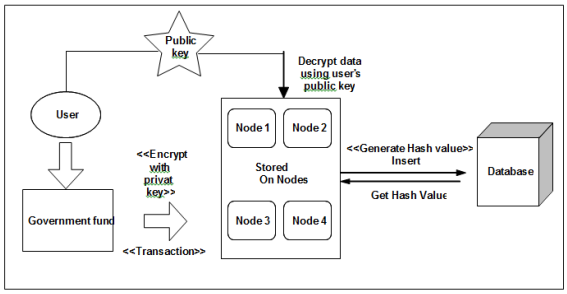


Fig.1 System Architecture

V.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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

Algorithm: Metadata file decryption

Data: Ciphertext CT, Cipher key CK

Result: File F

1. setKey(CK);

2. CipherTransform Secure Cipher CipherTransform.getInstanc ("AES/ECB/PKCS5Padding");

3. SecureCipher.init (CipherTransform.DECRYPT_MODE, CK);

4. F = SecureCipher.doFinal (Base64.getDecoder().decode(CT)

5. return F

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 a 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 wellknown (AES). it's far located at the least six times faster than triple DES.

A 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

AES algorithm:

Input: 128 bit/192 bit/256 bit input (0,1)
Secret key (128 bit) + plain text (128 bit).

Output: cipher text (128 bit).
Steps

1. 10/12/14-rounds for:128 bit /192 bit256 bit input
2. Xor state block (i/p)
3. Final round:10,12,14

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

5. Secure Hashing Algorithm (SHA)

Logic:

The algorithm takes as input a message with a maximum length of less than 2128 bits and produces as output a 512-bit message digest.
The input is processed in 1024-bit blocks. Fig 2 depicts the overall processing of a message to produce a digest.

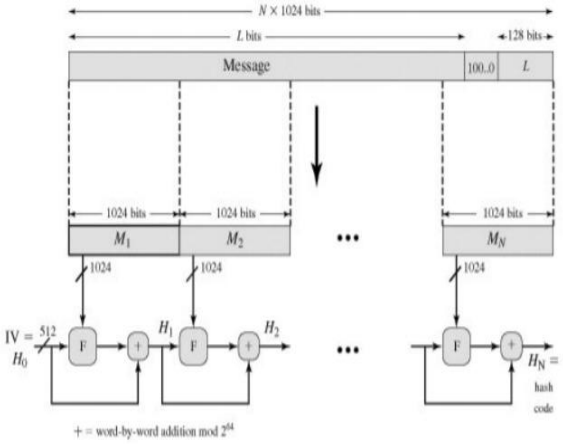


Fig. 2 Message Digest Generation using SHA-512

The processing consists of the following steps:

Step 1: Append padding bits:
The message is padded so that its length is congruent to 896 modulo 1024 [length 896 (mod 1024)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024. The padding consists of a single 1-bit followed by the necessary number of 0-bits.

Step 2: Append length:
A block of 128 bits is appended to the message.
This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding).
The outcome of the first two steps yields a message that is an integer multiple of 1024 bits in length.
In Figure 3, the expanded message is represented as the sequence of 1024-bit blocks M1, M2,..., MN, so that the total length of the expanded message is N x 1024 bits.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

Step 3: Initialize hash buffer:
A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers (hexadecimal values):
a = 6A09E667F3BCC908
b = BB67AE8584CAA73B
c = 3C6EF372FE94F82B
d = A54FF53A5F1D36F1
e = 510E527FADE682D1
f = 9B05688C2B3E6C1F
g = 1F83D9ABFB41BD6B
h = 5BE0CDI9137E2179
These values are stored in big-endianformat, which is the most significant byte of a word in the low-address (leftmost) byte position. These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

Step 4: Process message in 1024-bit (128-word) blocks:
The heart of the algorithm is a module that consists of 80 rounds; this module is labeled F in Figure 2 The logic is illustrated in Figure 3.

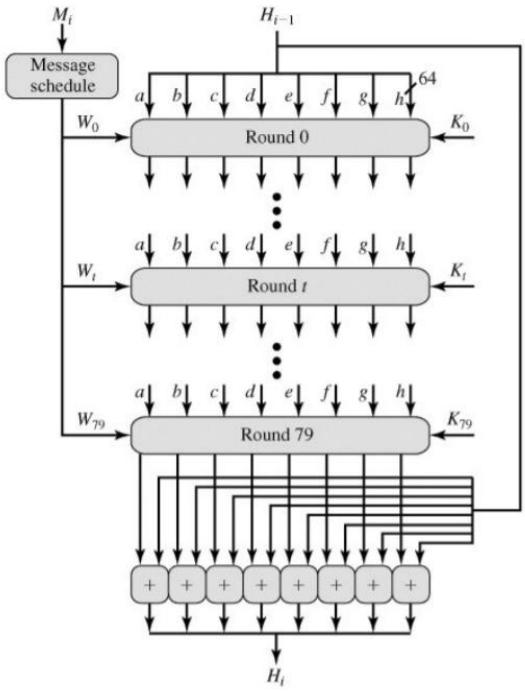


Fig.3 SHA-512 Processing of a Single 1024-Bit Block

Each round takes as input the 512-bit buffer value abcdefgh, and updates the contents of the buffer. At input to the first round, the buffer has the value of the intermediate hash value, Hi-1. Each round t makes use of a 64-bit value Wt derived from the current 1024-bit block being processed (Mi) These values are derived using a message schedule described subsequently.
Each round also makes use of an additive constant Kt where 0 t 79 indicates one of the 80 rounds. These words represent the first sixty-four bits of the fractional parts of the cube roots of the first eighty prime numbers. The constants provide a "randomized" set of 64-bit patterns, which should eliminate any regularities in the input data. The output of the eightieth round is added to the input to the first round (Hi-1)to produce Hi. The addition is done independently for each of the eight words in the buffer with each of the corresponding words in Hi-1 using addition modulo 264.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

Step 5: Output:
After all N 1024-bit blocks have been processed, the output from the Nth stage is the 512-bit message digest. We can summarize the behavior of SHA-512 as follows: H0 = IV Hi = SUM64(Hi-1, abcdefghi) MD = HN where IV = initial value of the abcdefgh buffer, defined in step 3 abcdefghi = the output of the last round of processing of the ith message block N = the number of blocks in the message (including padding and length fields) SUM64 = Addition modulo 264 performed separately on each word of the pair of inputs MD = final message digest value.

VI.RESULT

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.

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, anyoneand everyone can find out how the money is being used. Such a blockchain will surely reduce the ongoingcorruption 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. AntoniosLitke, DimosthenisAnagnostopoulos, 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, MengJooEr,“Tracking-Error-Based Universal Adaptive FuzzyControl for Output Tracking of Nonlinear Systemwith Completely Unknown Dynamics” ,*IEEE*APRIL 2017.
8. Adam Ghandar, ZbigniewMichalewicz, 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905243 |

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:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details