Block Chain for Secure Energy Trading on Solar System

Sheetal P. Shrotri, Prasad S. Halgaonkar

Abstract: ***Data security is progressively essential for generally organizations what's more, even home PC clients. Proposed framework will give the security to close planetary system information security utilizing blockchain idea. P2P network will used to store every owner solar based energy information month to month. All information identified with solar based energy information will be valuable and give the security of that information to avoid programmers and information lost for secure transaction. To avoid loss of information and its accessibility cryptographic methods are utilized. What the transaction information with any missteps will found and redressed before producing any block. To get accessibility and checked cryptographic hash are being placed in each block in the energy block chain. This framework deal with verification of - retrievability. Information store dependent on block chain security. The energy block chain conveys the hash value of past associated nodes to the consensus procedure and in the traditional block chain it applies consensus process on all node.***

Keywords: Block chain, Cryptography, Data security, Peer-to-peer, Proof-of- retrievability, Solar system

I. INTRODUCTION

The decentralized storage system presented with points of interest for capacity of server farms. Like the traditional arrangement, the non-centralized cloud distributed storage organize takes preferred standpoint of customer side encryption to maintain data security. Solar energy is a reliable and renewable source of energy, and it is additionally the cleanest kind of energy known to man, since it does not pollute and adds to the decrease of a nation's carbon emanations. A Block chain is list of records called block, that are associated by encryption. Each block has an exceptional hash of existing block and transaction data. By structure, a chain of blocks does not permit data modification. Blockchain is a distributed record that stores communication between two clients proficiently. To be utilized as a accounting book, a chain of blocks is generally handled by a machine to machine networks that delivers by protocol for correspondence among nodes and checks the new blocks. Once put away, the data in a given block can not be changed without evolving every resulting block, which requires the consent of the maximum of the network. The study of Blockchain in recent time is because of the decentralization advantage in the energy transaction.

Revised Manuscript Received on December 22, 2018.

Sheetal P. Shrotri, PG Student, Department of Computer Engineering, Zeal College of Engineering and Research, Narhe, Pune, India

Prasad S. Halgaonkar, Faculty, Department of Computer Engineering, Zeal College of Engineering and Research, Narhe, Pune, India

The open and distributed registry to keep verified and permanent transaction records is a blockchain. The chain of blocks in the consortium is a chain of coherent blocks with preselected nodes to keep the common databases appropriated. The chain of blocks of the consortium is mostly private. Here there has been some perplexity with respect to how this contrasts from a totally private framework. Rather than every individual inside System taking an interest in the verification of the transaction process or permitting just a single organization's individual that one have full control, some chosen nodes are predetermined. A consortium stage offers a considerable lot of similar advantages related with the chain of private blocks: efficiency and privacy of transaction

II. RELATED WORK

1. The record exhibited to diminish the transaction impediment is the consequence of postponements in the affirmation of the transaction in the chain of energy blocks. This framework offers an installment plot dependent on layaway. In the base cost procedure the advance depends using a credit card utilized by the Stackelberg diversion. In this Propose framework the stackleberg game is utilized in energy advances to increase the advantages of the credit banks. The assessment of execution examination and security of energy blocks and installment plot by credit [1].
2. Offering task is a distributed power trading model that is utilized to purchase and sell power locally between PHEV in keen networks. In existing frameworks transportation of power for long separations through complex transportation system of power. The proposed framework answers the question by giving motivators to the release of PHEV to adjust the nearby interest for power with individual interests [2].
3. In this work, proposed another IoT server platform for chain of blocks and presentation of sensor information storage into chain of blocks. The chose mobius IoT server stage to enable verification to IoT gadgets with good M2M standard for certain measure of time. It get sensor information what's more, data progressively from them and store it on the Mysql database server and controls them [3], [13].
4. In this work creator manage the issue of transaction security in shrewd lattice energy exchanging without provoke to other people. They have dealt with a proof of-concept in block chain innovation by utilizing multi-signature and encrypted informing [4].

5. In this work, they connected Zero Knowledge verification to a smart meter system for security assurance for without disclosing data, for example, public key[5].
6. In this archive, author have presented new distributed agreement instructions and guidelines for blockchain without a grant called ELASTIC. Versatile scales transaction speed linearly with the calculation accessible for mining: the more noteworthy the computing power in the system, the more prominent the number of transaction blocks chose per unit of time[6].
7. In this archive, author describes an access control driver dependent on a chain of blocks for clinical records that would propel the interoperability challenges of the sector expressed in the National Shared Interoperability Roadmap of the Office of the National Technology Coordinator. information[7].
8. In this archive, by utilizing distributed energy resources in energy the executivesplot for a keen network in residential units to a controller of shared services. The Stackelberg non-cooperative game between the UK and the CFS intends to works on utilities their energy trade between them[8].
9. In this work, they propose a protected and dependable strategy to secure the mobile communication, in which correspondence data duplicates are encrypted to disribute also, storage in every mobile terminal after validation [9].
10. In this record, they portray a decentralized private data the management system that gives clients control and ownership of the data. Author Implements a protocol for to transform the blocks under a automated access control of administrator without trusting to outsider. This framework permits putting away also, sharing instruction or information instead of money related transactions [10].
11. This work introduces another distributed energy trade framework between electric vehicles, which diminishes the effect of the charging procedure on the fuel framework amid working hours [11],[12].

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

Proposed work will provide the security solar system data utilizing block chain idea. This System will put away or transform the significant solar data on nodes in encoded format by utilizing private secret key utilizing block chain idea. The data will be encrypted utilizing cryptographic AES encryption method. The data can be specific clients articulation of cash claimed for energy services rendered. For these data this System will create the unique discrete token value to each node for security reason. So utilizing these techniques will be proficient and compelling to perform secure transaction on solar system data and give the security. Administrator will store every proprietor's solar data record of month to month utilized. The uploaded record will store on numerous node .All storage point of interest will store on blocks with hashing of detail. The encryption of document depends on keysetup, extract key encryption and decryption. MD5 is utilized for checking data store on all node is tempered or not while getting file from node to administrator. The consortium block chain transaction is digitally signed and it is to confirm that the non-validated person cannot change the nodes which lead to fizzle the network. In proposed framework non approved can't change a digital signature of every node, or to get control on the systems assets. In the consensus procedure before including the transaction records into blockchain, first discover off-base data from them and correct it.

In energy block chain the audit is required for all authenticated nodes and new node to check every transaction records in certain measure of time is called as transaction verification time, to finish the consensus procedure. Making Blocks in Energy Blockchain System get all transaction records after some periodic time are encrypted and digitally signed at that point these records to be authenticated. The transaction records are organized into blocks. For security and verification of each blocks in energy blockchain has a unique hash of past blocks.

In proposed system data deduplication is performed to reduce storage room of proposed system application use. Each time new record is uploaded and that entry is put away in blockchain. In the event that same data happens then likewise that data will be put away so here increase storage space. To reduce this system utilizes data deduplication application with MD5 Algorithm. That creates hash of data contained in file and put away in database. Assuming new data record is coming system discover MD5 Hash of that document if that is same at that point indexing will perform to past coordinated hash file. Also, when proprietor need this file he will get his file as per uploaded substance.

Module

1. user first register account in to application.
2. user login to system.
3. user upload the file .
4. user view all file .
5. user delete the file.
6. user get the file.

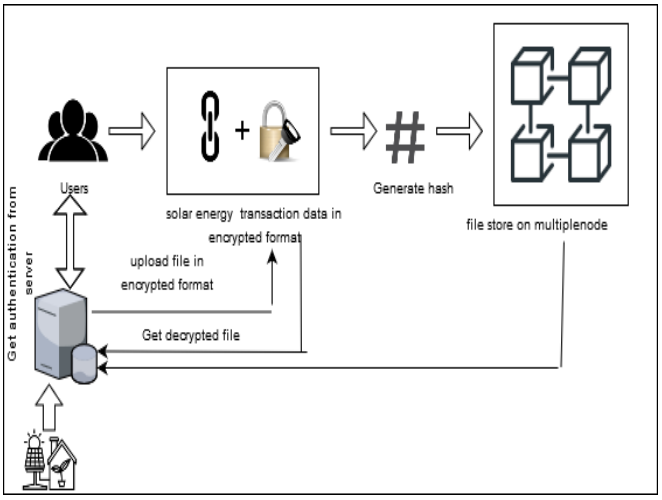

Fig. 1 Proposed System Architecture

Algorithms

Advanced encryption standard (AES) Algorithm For Encryption

It is symmetric Algorithm. It used to change over plain content into cipher text. The proposed framework utilizes AES Encryption algorithm. There are three variants of AES based on different key sizes (128, 192, and 256 bits). In proposed system we modifying AES key that administrator will upload the file and that file will encoded with AES. The key for AES will be crated by Owner emailid, current time called quality based key. This attributes are consolidated and private key will produce as indicated by that and with this key encryption will be occur. For that we will use keyGenerator class.

Steps

Encryption

Step 1: Generate attribute based key with emailed of bill owner and current time. Step 2: Combine key and plaintext.
Step 3:AES Round : each round consist of four steps
1. Substitute bytes, 2. Shift rows, 3. Mix columns, and
4. Add round key.
Step 4: Encrypted data.

Decryption

Step 1: Pass Generated attribute based key with emailed of bill owner and current time. Step 2: Combine key and cipher text.
Step 3: AES Round for decryption Step 4: Plain text data.

MD5 Algorithm

The message digest 5 algorithm accept input in the form of message. The message length can be vary and the yield delivered in 128 bit finger print or message digest of the input message. It is computationally impossible to deliver same message digest for two messages. It performs quickly on 32-bit machine.

MD5 is considered one of the most efficient algorithm at present accessible. Consider input as b-bit message, and then following steps is useful to find out message digest of its input. In proposed system MD5 is utilized in putting away information.
Algorithm: DE duplication checking for data storage.

Steps

Step 1: Select the file which to upload.
Step 2: calculate hash=md5(data) of uploaded file.
Step 3: compare hash of selected file that going to uploading with already stored all file.
Step 4: If hash is matched with previous any file go to next step else go to 7 Step 5: Provide index(matched file)
Step 6: Store index reference of file for newly uploaded file.
Step 7: upload new file
Step 8: calculate hash=md5(data) and store in db.

Mathematical Model

A block cipher is specified by an encryption function File uploading

File uploading

$E_k\,(P)$: = $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

In this equation inputs taken are:

Key K for key size of bit length k called the key size, get attribute based key emailidof bill owner and current time.

P used for block size of n length bit string

C called cipher text which returns a string C of n bits. P is called the plaintext,

File downloading

$E^{-1}(c)$: = $D(k, c) : \{0, k\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

For each K, the function EK(P) is required to be an invertible mapping on 0,1n. The inverse for E is defined as a function

key K and a ciphertext C to return a plaintext value P, such that

$\forall K : D_k\,(\,E_k\,(P))$ = $PallK : D_k\,(\,E_k\,(P)) = P$

Access Control

Access control is kept up by checking consensus process of each block with the MD5 Hash checking.

It check hash=md5(data) with each block. If selected node giving result true for each past block then just can new data will get admittance to enter in new block. The consensus procedure will execute In that procedure just selected blocks results are considered

Lets take a Block b11,b12..b1n for record f1.

H(b11), H(b12).. H(b1n) for including new record of same client

Block b21,b22..b2n for record f2 H(b21), H(b22).. H(b2n) will included if b11,b13,b15 selected blocks give genuine value this is selected blocks accord process .It will decrease time of our system.

Check all previous selected blocks chain hash value result is valid for all block then just blocks of new file will included.

Hardware and Software requirements

Hardware Requirements

1) Processor - Intel i5 core
2) Speed - 1.1GHz
3) RAM - 2GB
4) Hard Disk - 40GB
5) Key Board - Standard Keyboard
6) Mouse - Optical Mouse
7) Monitor - SVGA

Software Requirements

1) Operating System - Windows7/8/10
2) Coding language - Java, MVC, JSP, HTML, CSS etc
3) Software - JDK1.7
4) Tool - Eclipse Luna
5) Server - Apache Tomcat 7.0
6) Database - MySQL 5.0

IV. SYSTEM ANALYSIS AND RESULT

Experimental setup Table 1-indicates showed the execution correlation for transaction confirmation. Fig.2- Shows a pictorial portrayal of execution correlation for transaction confirmation. X-node recurrence of energy exchanging and y-node for absolute transaction affirmation time of one node.

The accompanying table demonstrates the execution correlation of the complete transaction affirmation time. The normal time to complete the consensus procedure in a energy trading of a specific node is known as the all-out transaction adaptation time. The energy block chain conveys the consensus procedure of preselected associated nodes and in the traditional block chain it applies consensus process on all node.

Table. 1 Performance comparison for transaction confirmation

Index Number	Traditional block chain	Proposed block chain
1	7	55
2	12	125
3	37	180
4	40	250
5	45	310

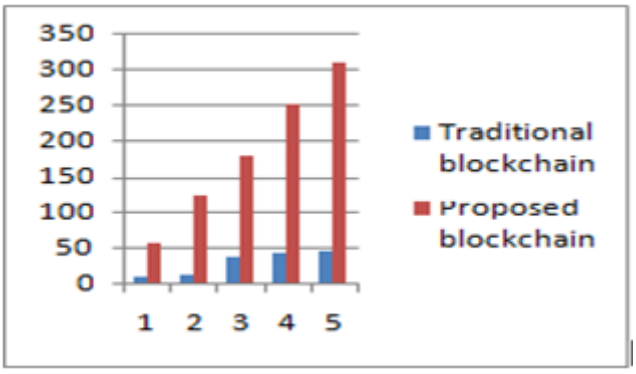

Figure 2. Representation of performance comparison for transaction confirmation

V. CONCLUSION

Introduced a block chain based system for secure energy exchanging solar energy data. The data will be effectively encrypted utilizing AES encryption system. Data storage and its outsourcing to service provider distributed network is permitted by this system. So that any unapproved individual does not permit any kind of change in the audited, put away data in the energy block chain. The system makes utilization of block chain technology to enforce the data trustworthiness through proof- of-retrievability scheme with hashing techniques. This system will be exceptionally proficient and viable to perform secure transaction on solar system data. A lot increasingly complex necessities like credential revocation and Boolean keyword search required in future work. Data store based on block chain security. The energy blockchain carries the consensus process on the preselected nodes in the existing block chain system.

REFERENCES

1. Zhetao Li , Member, IEEE, Jiawen Kang , Rong Yu , Member, IEEE, Dongdong Ye, Qingyong Deng , and Yan Zhang , Senior Member, IEEEConsortium Blockchain for Secure Energy Trading in Industrial Internet of Things- IEEE Transactions on Industrial Informatics, Vol. 14, no. 8, August .
2. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybridelectric vehicles using consortium blockchains IEEE Trans. Ind. Informat.,vol. 13, no. 6, pp. 31543164, Dec. 2017.
3. Jin Hyeong Jeon, Ki-Hyung Kim, Block chain based data security enhanced IoT Server Platform. 2018 International Conference on Information Networking (ICOIN)
4. N. Z. Aitzhan and D. Svetinovic, Security and privacy in decentralized energy trading through multi- signatures, block chain and anonymous messaging streams, IEEE Trans. Depend. Sec. Comput., to be published, doi: 10.1109/TDSC.2016.2616861.
5. Chan Hyeok Lee, Ki-Hyung Kim, Implementation of IoT System using Block Chain with Authentication and Data Protection. 2018 International Conference on Information Networking (ICOIN)
6. L. Luu et al., A secure sharding protocol for open blockchains, Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 1730.
7. L. A. Linn et al., Blockchain for health data and its potential use in health it and health care related research, ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, USA: ONC/NIST, 2016.
8. W. Tushar et al., Three-party energy management with distributed energy resources in smart grid, IEEE Trans. Ind. Electron., vol. 62, no. 4, pp. 24872498, Apr. 2015.
9. Liufei Chen, Yushan Lo, Hong Wen, WenXin Lei, WenJing Hou, Jie Chen, Block Chain Based Secure Scheme for Mobile Communication. 2018 IEEE Conference on Communications and Network Security (CNS)
10. G. Zyskind et al., Decentralizing privacy: Using block chain to protect personal data, in Proc. IEEE Security PrivacyWorkshops, 2015, pp. 180 184.
11. R. Alvaro-Herman, 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. 3344, Fall 2016Formatting your Paper
12. PS Halgaonkar, S Jain, VM Wadhai, NFC: A review of technology, tags, applications and security, International Journal of Research in Computer and communication Technology, 2013
13. Poonam M Bhagat, Prasad S Halgaonkar, Vijay M Wadhai, Comparison of LTE and WiMAX on the Basis of Qualities, International Journal of P2P Network Trends and Technology,2011.