ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Smart Transportation System for Data Security in Blockchain

Varsha Amol Abhang, Smita Bhosale

Asst. Professor, Department of Information Technology, Sinhgad College of Engineering, Vadgaon Pune, India

Asst. Professor, Department of Computer Engineering, Sinhgad Institute of Technology and Science Narhe, Pune, India

ABSTRACT: In today's life production industries growing that consist transportation. In block-chain technology, each page in a ledger of transactions forms a block. That block has an effect on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or block-chain. In proposed system data will be of transportation data need to secure. This work is designed using block chain concept and key-based cryptographic technique. Stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then compares the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. Proposed system work on storing data of transportation. This system will work on consensus mechanism while adding data in blockchain. This system will find malicious users and inform to owner.The uploaded data file will replicate based on T-Coloring concept of node for data placement.

KEYWORDS-Block, Block-chain technology, ledger, cryptography, hashing, transportation system storage data.

I. INTRODUCTION

Block-chain is an emerging technology for distributed and transactional data sharing across a large network of un-trusted participants. In today’s day in industry production is growing fast also as well as the product need to transfer at dealer .Manager of company will store transportation’s data securely.It allows new forms of distributed software architectures. Although the technology was mainly accepted in digital currency in initial days, but it is a promising technology for other areas too. This work is designed using block chain concept and key-based cryptographic technique. Stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then compares the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. Proposed system work on storing data of transportation. Blockchain is a novel decentralized ledger-based storage method. Satoshi firstly applied Blockchain into Bitcoin, which is a peer to peer e-cash system. Later, Blockchain gets more and more attention in e-commerce. Particularly, it has become a hot topic since Blockchain-based Bitcoin became popular. Moreover, in Blockchain-based networks, each node manages a copy of the whole or part of a database from the system. Thus, Blockchain-based networks are promising in recording credit data with the good properties of tamper resistance and decentralization, which is useful in VANETs. Tree Signature is widely used in public key cryptosystems. Merkle firstly proposed Tree Signature as a digital signature authentication. Because of the lower storage cost and the efficient verification, Merkle Hash Tree was used in the construction of cryptography in , in order to create the hash index of transaction records and the verification of data.

1.1 MOTIVATION

Block-chain is an emerging technology for distributed and transactional data sharing across a large network of un-trusted participants. In today's day in industry production is growing fast also as well as the product need to transfer at dealer .Manager of company will store transportations data securely . It allows new forms of distributed software

DOI: 10.15680/IJIRCCE.2019. 0703038

architectures. Although the technology was mainly accepted in digital currency in initial days, but it is a promising technology for other areas too

II. REVIEW OF LITERATURE

1. R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens Present the concept between two agreements of electric vehicles, which substantially reduce the effect of the loading procedure on the power structure in the middle of working hours. This commercial approach is also economically beneficial for all users involved in the negotiation process. An activity-based approach is used to predict the daily schedule and travel of a synthetic population for Flanders [1].

2. Y. Xiao, D. Niyato, P. Wang, and Z. Han Provide a study of the possible flow and functional factors that allow DET in communication networks. Several design problems are discussed on how to implement DET in practice. An ideal approach has been created for paired and radio-tolerant correspondence organizations in which each remote device can dominate its information transmission and energy exchange activities as indicated by the accessibility to present and future viability [2].

3. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a job to complete the reaction request by providing motivating forces to free PHEV to match the demand for power close to his personal interests. However, given that security and safety issues show real difficulties, they investigate a promising chain link innovation in the consortium to improve the security of the exchange without relying on an unknown confidant. A P2P electricity negotiation framework is proposed with a consortium chain block strategy to represent limited detailed P2P energy exchange activities [3].

4. N. Z. Aitzhan and D. Svetinovic presents a paper that addresses the problem of providing transaction security in the decentralized energy trade of smart grids without trusting reliable third parties. We have developed a proof of concept for the decentralized energy trading system using blockchain, multiple signatures and encrypted anonymous message flows, allowing peers to anonymously negotiate energy prices and conduct business transactions safely [4].

5. M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now presents a work that shows computerized decentralized money, called the NRG currency. Prosumers in the framework of smart grid exchange have sustainable energy sources created privately using NRG currencies, whose estimation is irregular in an open cash trade. Like the Bit currencies, this money proposes several favorable circumstances with respect to money in fiduciary currency, but not very similar to the bit currencies that are produced by infusing vitality into the matrix, instead of giving vitality to the computational influence. They also make a novel that exchanges the vision of the world for the purchase and supply of vital ecological energy in the network of smart grids[5].

6. 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].

7. 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 currency reference design [7**].**

8. K. Croman et al presents a work that the growing fame of digital forms based on the chain of blocks has made versatility an essential and serious obligation. The work reflects how the essential and accidental Bit-coin bottlenecks limit the capacity of their current distributed overlay system to help generate generically greater and lesser latencies. These results suggest that the re-parameterization of the square dimensions and the interruption should be considered only as a first step to reach people, the conventions of the chain of high-stacking blocks and true progress will also require a fundamental re-evaluation of the forms specialized
[8].

9. 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

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].\\

10. L. Luu et al presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO is productive in its system messages and permit complex foes of up to one-fourth of the aggregate computational power [10].

III. PROPOSED METHODOLOGY

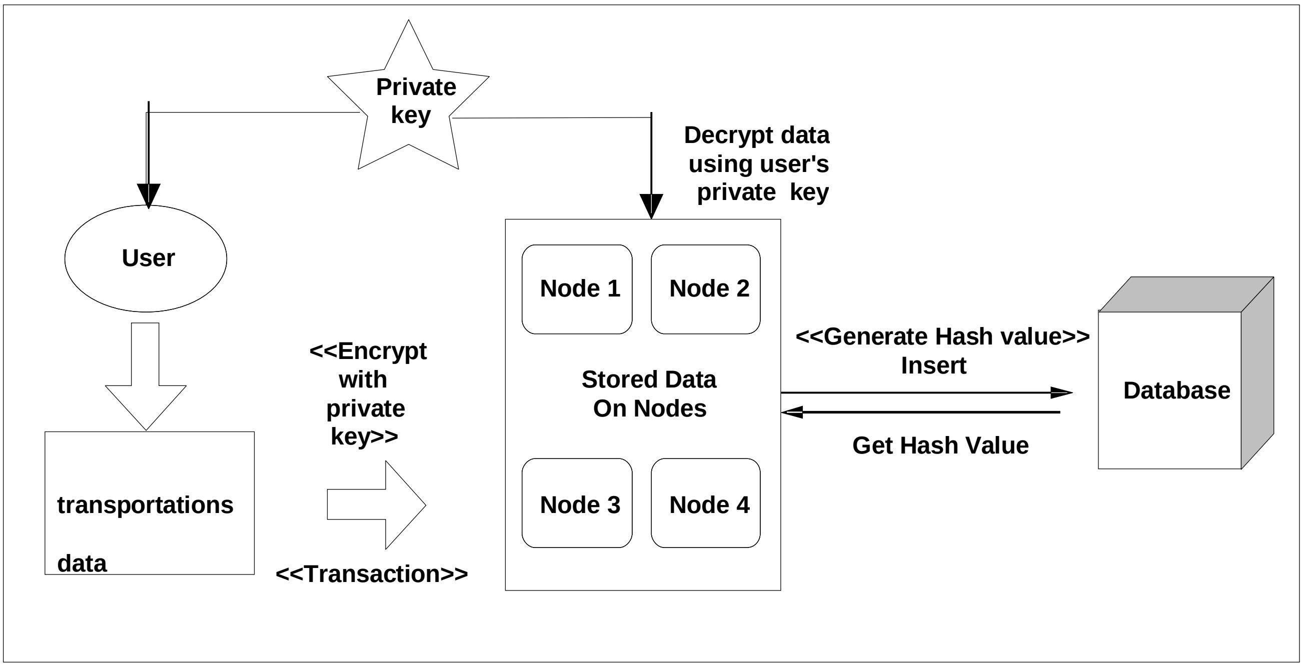

Fig.1: System architecture

SYSTEM OVERVIEW

Data forms the foundation of the application system, and its integrity is the key to the data's value and the aim of data security technology prevention. According to the approach of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, normally appended to the data file. In general, the intension of using a private key-based cryptography technique is for recipients or users to verify the origin of the data information. For data security, this work is designed using block chain concept and hash signature technology. In this work we stores the hash tables of raw data and files on the block-chain, validates other copies by running a hashing technique, and then checks the data stored in the block-chain, any interfere with the data will be quickly found, because the original hash Tables are stored on millions of nodes. In this company manager will store transportation data for different dealers. The requests, announcements, and the transactions do not leak any information about their sources The announcements are signed by several honest witnesses (truthfulness). According to threshold authentication and Blockchain, every user could manage a copy of the whole block chains of transactions, and each transaction is related to the phases of announcement aggregation. Therefore, a source is unable to deny sending messages (non-reputation). Additionally, announcements and transactions cannot be modified without authorization (tamper-resistance). Merkle Hash Tree is a binary tree, and each leaf node is related to a fixed hash value calculated from a small fixed fragment. In other words, each leaf node represents a unique and fixed fragment. The union set of all fragments is made up by raw data waiting to be verified. The hash value of a parent node is computed by the hash value of its child node. As the raw data and the fragment are fixed, the root of the hash tree is also fixed. Thus, the verification of a fragment is the proof of the existence of a leaf node. This is proceeded by finding a path from the fragment to the root. The consensus server is an entity that receives transactions and participates in the consensus phase.Uploaded file will place on node concept of T-Coloring.

IV. MATHEMATIAL MODEL

This T-coloring concept will be applicable while uploading data on node the file will replicate on nodes and the node selection process will be based on T-Coloring concept.File will placed and its replica will place at non-adjacent node based on T-coloring concept.In simple words, the absolute value of the difference between two colors of adjacent vertices must not belong to fixed set T. The concept was introduced by William K. Hale. If T = {0} it reduces to common vertex coloring.

V. ALGORITHM

1. Advanced encryption standard (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 as weak.

```
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 bit\/256 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.\\
```

SHA-1(Secure Hash)

This algorithm will used for generating hash of transaction data. This will be used in consensus mechanism.

In cryptography, SHA-1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they are transformed into their respective hash values, its virtually impossible to transform them back into the original data. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific users hash value, rather than the actual password.

VI. RESULT

Experimental setup Table 1-gives the information of uploading time for 30kb, 50kb, 100kb, 1mb and 3mb file size.Fig.2- size of file and time to upload that file after performing fragment and t-coloring .As size of file increases the time will increase.X-axis size of file and y- Time to upload in ms.The file will replicated based on T-coloring concept.

DOI: 10.15680/IJIRCCE.2019. 0703038

Index Number	File size	Time in ms
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table01: shows file size and time in ms

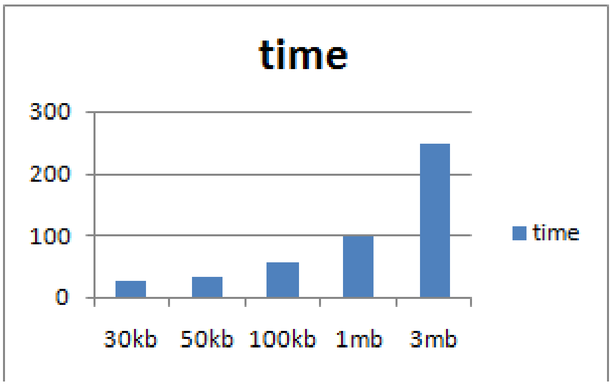

Fig. 2. Shows file size on x axis and time (ms)to upload on Y-axis

VII. CONCLUSION

In work is designed using block chain concept and cryptography technique which estimate the security of block-chains specifically using hashing. Proposed system work to security on transportation data. Block-chain technology is not just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes. This work is designed using block chain concept and cryptography technology to provide the security to transportation data of vehicle and product. It maintains the reliability and anonymity of the data simultaneously.

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.

78. 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.