Securing data sharing Track Record in a network using Blockchain Technology

Prince Kurian[1]

[1] *Assistant Professor,Information Technology Department,Viswajyothi College of Engineering&Technology,Vazhakulam,Kerala,India*

ABSTRACT

Now a day's tremendous amount of data is being shared among the network. We can secure the data by using some encryption techniques, so that a third party can't able to read or modify the original data. In a global network there may be millions of computers participating in a data sharing or message sharing at the same time. We need to keep a record of who send the message, to whom it is sending and when it is sent. This is a vital information and later it may be very useful for tacking the origin of the message. In current systems like WhatsApp or any other social media this information is stored in their server machines. But if the central machine crashes the entire information's will be lost or any hacker modified any information in the central machines it is very difficult to recognize the modification and recovering. Or in other words we can't trust a single machine to store confidential information. In this scenario we can use Blockchain Technology to store the history of data sharing with more secure and unhackable

Keyword - *DBMS, blockchain, security*

Introduction

In the world of networking each and every second a new data is getting created and shared among different data sharing applications and different social networking sites. After it is shared, it is very difficult to find who created that data and who all are the intermediate nodes passed the data to the next node. So the history of the data - from the origin to current node holding the data-should be stored safely and securely. If are storing that information in a central server there may have so many problems regarding the security and authenticity like (i)If the machine crashes all information's will be lost (ii)If any one updates the data ,then it is very difficult to find updates happened. In this scenario it is better to use blockchain technology to store such information, because in this technology there is no central server to control the system, but all the nodes participating in the network have equal responsibilities to ensure the security and authenticity. If anyone tries to modify the data, it is very easily get recognized and resolved. So in this technique we can ensure security, safety and authentication.

How it Works?

We need to keep track the history of messages being sent, who is the creator, who is forwarding to whom etc. The technology behind the problem is blockchain .Blockchain is a collection of blocks and each block contains different valid transaction details. If there are 'n' different nodes involved in the network, then each node having same copy of the block chain. So the information regarding any transaction will not be lost at any point of time. If any node trying to modify any blocks in a block chain, it will be easily detected by nearby nodes. The blockchain technology uses the concept of hashing and public key encryption to maintain integrity and confidentiality of the block. Suppose node 'A' wants to send money to node 'B', then node 'A' has to prepare this transaction details and send all the nodes in the network. The nearby nodes can easily verify this transaction is valid or node 'A' have enough money to transfer, because all node have a valid block chain contains all transactions of all nodes. If all nodes saying it is a valid transaction and node 'A' having enough money to transfer then this transaction is recorded and added to a block. This verification will take around 10 minutes and if majority of nodes saying its valid then it transaction will added to a Block .In the meantime there may be thousands of transaction taking place around the world. For every 10 minutes it will create a new block and all the valid transactions during that time is added to that

block. Then the validity of this block is checked by special nodes called 'miners'. It is the function of a miner to find the block the miner added this block to the existing block chain. And this block chain is published in the network. The first miner who finds the valid block will reward with some bitcoin.

Security Measures of Block chaining

1. Blockchain

A Blockchain is a chain of blocks. This blockchain is stored in all the nodes participated in the network. So the consistency of the blockchain is guaranteed. If any node tried to modify data in the block chain, it can be easily detected because all nearby nodes having the original copy of block chain. So blockchain itself is consistent. If anyone wants to alter data in a blockchain first he has to update his own blockchain and alter blockchain of all other nodes in the network. This is practically impossible to alter data stored in all other nodes, because there may be millions of nodes available in the network. If any node contains a mismatched blockchain the system will check this blockchain with others and the blockchain with majority node have been accepted. So the modification of blockchain is impossible [1].Blockchain doesn't require any third party to check the consistency; the system itself can check its consistency.

2. Blocks

The main important part of blockchain is blocks. This blocks contains all transaction details that happened during 10 minutes of time. Each block contains different values such as transaction details, hash value of previous block, hash value of the block, timestamp, index etc.

In each 10 minutes of time, there may be thousands of valid transactions taking place, and all these transactions are entered into a newly created block. Then this block is added to the block chain and this blockchain is published in the network.

Each block is secured by adding a hash value at the end of the block. If a single character change in the block will result an entirely different hash value. Blockchain uses SHA-256 hashing algorithm for hashing. Each block contains hash value of its own block and hash value of the previous block. If any node tries to modify the values in a block, then the hash value of the block will change .So this can be easily detected by the system because, original hash value is stored in the next block also. If he really wants to update/modify any values in a block, then he need to modify all blocks in a blockchain, because hash value of a block is stored in the next block also. It is really impractical. If he succeed in modify all blocks in a blockchain, he may get a valid blockchain. But the system can detect the modified blockchain because the original blockchain is stored in all other nodes in the network. So modification of a single value in a block is impossible.

3. Transaction

Each block in a blockchain contains another important field of transaction details. The transaction detail contains the information like, who send the money, to whom it is sending, how much amount being transferred etc [5]. This is a very sensitive data so that no one should alter. Suppose node 'A' wants to send 2BTC to node 'B', then this transaction should satisfy following criteria's.(i)Transaction should not be altered by any third party node (ii) node 'B' should ensure that sender is node 'A'. (iii) Node 'A' should ensure it is received by node 'B'. To ensure all this properties transaction uses the concept of digital signature. To digitally sign the transaction details, the system uses asymmetric encryption that uses public key and private keys. And to ensure the integrity of the transaction it uses hashing also as shown in Fig 1 [1].

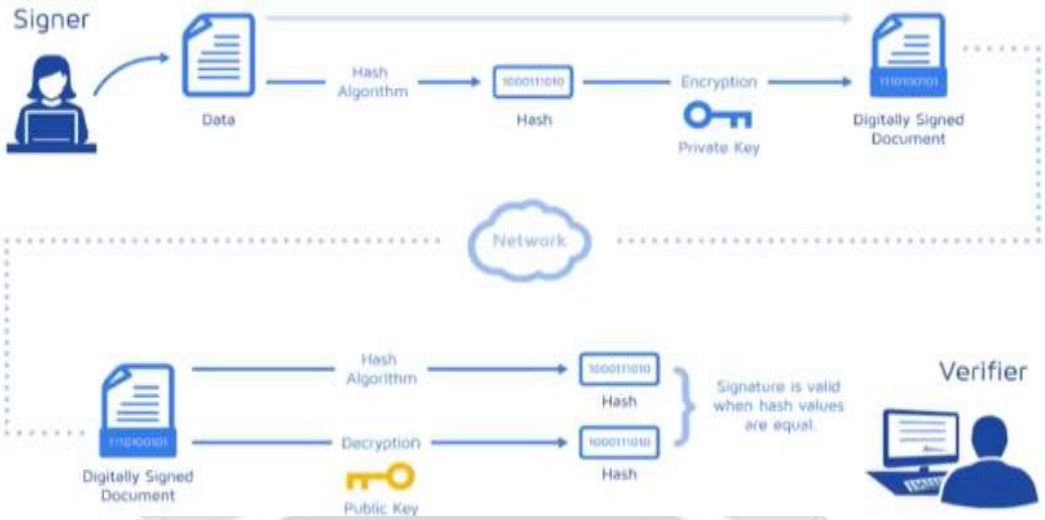

Fig 1: Transaction stages between two nodes

The sender sends the transaction details to the receiver only after digitally sign the document. To sign the document sender first apply hash function to the document to ensure integrity and later encrypt the result by his own private key. The receiver can decrypt the document with senders public key ensuring sender is the real sender. Then the receiver has to check integrity of the massage .After decrypting he will get a hash value. This hash value and received document hashed value has to be compared to ensure the integrity of the transaction. If both the values are same then we can ensure that no one altered the transaction.

So each transaction in the blocks in a blockchain is secure and safe. No one can alter any value in the transaction. If any node altered the values in a transaction, then the hash value will change at receiving end. So the receiver can easily identify the integrity of the transaction. Such transaction will not be added to the block. So only valid transactions will be there in a block in a blockchain.

Conclusion:

It is very crucial thing to keep track a message in the network such as who created, from which node to which node it is passing and current status of that message. To keep track such information, we can make use of this technology blockchain. With this technology we can ensure highly secure data and the available track record will not at any point of time. This method is highly secure, confidential, authentic and unhackable.

References:

1. www.edureka.co/blog/blockchain-tutorial [Accessed on 18-Dec-2017]
2. https://en.wikipedia.org/wiki/Bitcoin [Accessed on 18-Dec-2017]
3. https://bitcoin.org/en/ [Accessed on 18-Dec-2017]
4. Reid F, Harrigan M, "An Analysis of Anonymity in the Bitcoin System",2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT), Boston, MA, USA , 9-11 Oct. 2011.
5. Karame G, Androulaki E, Capkun S,"Double-Spending Fast Payments in Bitcoin", Proceedings of ACM CCS 2012.