

Decentralized Applications using Blockchain – Managing government corruption

S Gopi¹, M Prasanna², R Shijil³, S M Aslam⁴, M Prakash Kumar⁵

¹Assistant Professor, Department of IT, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai-600123, Tamil Nadu, India.

^{2,3,4,5}B.Tech., Department of IT, Panimalar Engineering College, Varadharajapuram, Poonamalle, Chennai-600123, Tamil Nadu, India.

Abstract - A Blockchain is a continuously growing record, called blocks, which are linked and secured using cryptography such as hashing. Each block contains a hash pointer as a link to the previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is similar to a ledger, but in this case, it is a distributed ledger which can record transactions between two different parties efficiently in a verifiable and permanent way. The data stored in the block is permanently stored and it cannot be modified or deleted. In this project using the blockchain technology can be used to store transactions taking place between the government and sensitive government data. In doing so there is more transparency in the data stored and thus it cannot be modified illegally. The blockchain is distributed to all the members who are using this system. Thus, whenever a block is added it is verified by all the members. Thus, this prevents people from illegally modifying government transaction or data thus stopping corruption to an extent.

Key Words: Blockchain, Bitcoin, Distributed ledger, Cryptographic hashing, Decentralized storage of sensitive data.

1. INTRODUCTION

We are living in a digital era where everything is digitised. We are dependent on technology to get our work done fast and efficiently. Most of the systems like file handling, management of transactions, business management etc., are all managed efficiently using technology. In the past file handling and management of transaction (transaction of money, business deals, corporation data etc.) were done manually and there was a problem of duplicate data which may lead to corruption of data. There was also double spending problem in banking system due to improper management of transaction data. All these transactions and management of data was done by a central server or a central system. Thus this may also lead to a risk in which loss of data occurs when the central server crashes. We overcame all these problems slowly using technology and digitized all these process. But still there are problems like duplication and corruption of data, illegal modification of data, money laundering etc. Since all the transaction and data handling process is done by a single body there is less trust placed on this system since there are ways in which people can tamper

with the data for their needs. Thus this had led to corruption of people and government, as sometimes there is no proof for the data being tampered or corrupted. To avoid all these problems as much possible we can use Blockchain technology to handle storage of sensitive data and to conduct transactions.

1.1 Need for this project

In present day there are lots of corruption taking place in government like illegal documentation, money laundering, alteration of sensitive data etc., Government members are altering transaction and fund data for their own needs and make profit out of it. Most of the profit is black money. Even after demonetization process which took place in India on 8 November 2016, there are still corruption and money laundering taking place. To reduce all these problems, we can use blockchain technology to handle the storage of sensitive files, data and transactions taking place between government system. As blockchain system is distributed in nature, everyone who is involved in using it, has all the data stored in the blockchain and thus even if a single person modifies the data illegally, we can verify that the data is altered. Thus, this helps in preventing future illegal alteration of sensitive data and thus corruption can be reduced.

1.2 Existing System

In the existing system of blockchain, all the transactions and the data stored in the blocks goes through Proof of work algorithm. A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required *on average* before a valid proof of work is generated. Transactions and data related to government are handled centrally by government organization which involve in certain people managing all the transactions and storage of sensitive data. Thus, there is a lot of probability for the data to be modified illegally which in return leads to corruption.

1.3 PROPOSED SYSTEM

Since the existing system has the drawbacks of consuming lots of time and resources for generating a specific hash value and it takes immense time for validation of the

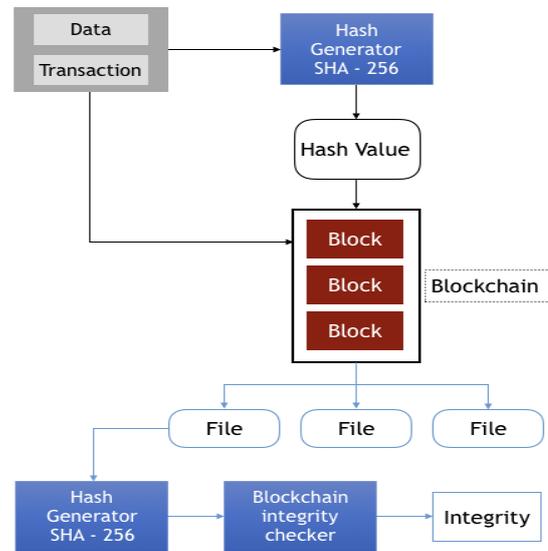
blockchain if a block is not valid or if the data has been modified. Thus, in the proposed system for every data the hash value is computed and stored. Whenever the transaction and the storage process in the blockchain is over, the blockchain is written into a separate file and the hash value for that file is computed and stored. Thus, the integrity of the file is checked before a block is added to it by generating the hash value for each blockchain files and comparing them. Thus, instead of comparing each hash value of the data stored in the blockchain we can compare the hash value of the file instead, thus saving time and computing resources.

In addition, the principles of blockchain is used in maintaining the integrity of the government transactions and in storage of sensitive data, where instead of handling the said processes by a single organization, we can decentralize the whole process where everyone who is involved in this have to contribute towards the integrity of the data stored in the blockchain. When ever a block is added, it is verified by the members involved in the transactions. All the transactions and data stored is stored along with its hash value and whenever someone tries to illegally modify the data for their own benefits, we can identify the change and we can stop it. Thus, there is a lot of transparency in the system. And thus, the corruption in the government over black money and money laundering can be stopped to an extent.

2. IMPLEMENTATION OF PROJECT

This project is completely implemented in JAVA programming language. The implementation is majorly focused on the storage process of the data and maintaining the integrity of the stored data in blockchain. Each data, along with its hash value is stored in the blockchain and the entire blockchain is stored in a file. This file is the file which is to be distributed along with the all the users with the files hash value. Whenever the integrity of the blockchain is to be checked, all the hash value of the blockchain file is recomputed and is compared with each other to check whether they are the same or not, thus checking the integrity of the blockchain.

2.1 PROPOSED SYSTEM ARCHITECTURE DIAGRAM



3. FUTURE ENHANCEMENTS

- Enhance the security of the system
- Support for storing multiple types of data and files
- Support for multiple storage technology
- Further improve the resources and time required for computing hash value

4. CONCLUSIONS

Thus, in this project we have studied about blockchain technology, its usage and its implementation. It is used majorly in Crypto currency, which involves in generating specific hash value for proof of work. This demands high computational power. As for this project the blockchain technology is used in conducting and storing government transactions so that it cannot be modified illegally to reduce corruption. This project provides the methods for storing data in blockchain as a file and maintaining its integrity by using the hash value generated for each file. By this method we can stop government corruption to an extent.

REFERENCES

- [1] Blockchain Technology as an enabler of service (Aug 2017) - Stefen Seebacher
- [2] Using Blockchain Technology to Validate the Integrity and Confidentiality of Backups Versions on the Cloud (Feb 2018) – Badr Aleidi, Abdulaziz Albeshar
- [3] A review of blockchain (Nov 2016) – George Pirlea
- [4] Blockchain platform with proof-of-work based on analog Hamiltonian optimizers (Feb 2018) – K. P. Kalinin.