**DR B.R. AMBEDKAR NATIONAL INSTITUTE OF**

**TECHNOLOGY JALANDHAR,**

**PUNJAB, INDIA**



**Final Year Project**

**Session: December-May 2020**

**TOPIC: BLOCKCHAIN FOR DIGITAL GOVERNMENT**

**MENTOR:-**

**Dr. Samayveer Singh**

**Assistant Professor**

**CSE Department**

**TEAM MEMBERS:-**

**Harpreet (17103035)**

**Prashant (17103061)**

**Rajnish (17103069)**

**Rupinderjit Kaur (17103075)**

1. PROBLEM STATEMENT

Government collects its finances from different revenue and capital means, which constitute the budget of the government for a financial year. This budget is then distributed among the various ministries and departments. The ministries and departments then further allocate the resources to various schemes projects and departments of lower levels. The money flows through various levels of the government and reaches the end where it is actually used in employing the services at the ground level.

This money distribution system lacks transparency, people at lower levels have no means to validate the exact amount of capital they were supposed to obtain. They only know what the officials on levels higher to them in the hierarchy have told them, which makes this system prone to corruption. When the people on the ground level do not get the sufficient resources, it has an adverse impact on the quality of services they provide and thus hindering the development in the country. As more government entities encounter budget shortfalls, maximizing revenue collection and reducing fraud become priorities.

The major causes of this problem are the lack of transparency, modifiability or corruption of records and the centralised bureaucratic system. This is where Blockchain will help us. Blockchain is a digital record of transactions made in cryptocurrency and maintained across several computers linked using Pair-to-Pair Network. It is a growing list of blocks containing the transactions data and time stamp, and the cryptographic hashes of the previous blocks. The blocks are also linked using cryptography.

We intend on automating the budget distribution system using blockchain. Such a system will have the following advantages:

* It will be a Decentralized System.
* The system will be Transparent.
* The system will be more Secure.
* The system will be Faster and Cost-Effective.
* The system will be Immutable.

Blockchain technology has a huge potential to iron out the glitches and improve efficiency in India’s Budget Distribution System. It can help us to increase transparency and curb corruption in the money flow through the various levels of the government from the top to the bottom of the distribution system.

1. LITERATURE STUDY

We have studied the following research papers of related works in ‘E-Governance using Blockchain’:

[1] presents research on Government Information Sharing Model using blockchain technology. The main goal of this research is promoting transformation of government affairs from management to service and building service-oriented e-government. The problem dealt is that the government software built and used during the imbalanced developed economy, technology and society and are requirements driven. It makes e-government systems have problems such as unclear positioning of information sharing mode, low degree of sharing customization, low security and the barn effect.

Blockchain comes in three forms, public blockchain, consortium blockchain and private blockchain. Consortium blockchain can be used by government agencies because it has the characteristics of decentralization and can guarantee access authorization. Within the consortium blockchain, information resources are jointly maintained by nodes, the entries and deletions do not affect the operation of the whole blockchain, at the same time, the consortium blockchain ensures that records in all nodes could not be tampered, as well as meeting the information sharing requirements of different government departments.

The barn effect can be broken as major corruption issues arise when information flow horizontally at level and not vertically. As we know blockchain technology has the characteristics of Peer to peer, the content of a node does not affect the other nodes, at the same time use of consensus plugin guarantees the data synchronization, and consistency of algorithm will keep the data safe.

Digital contracts and digital seals built has government data protected using the Secure Hash Algorithm(SHA) to prevent the tampering of the information content. That means even before adding the data to a blockchain node, the data will be encrypted to ensure the legitimacy of the data.

Government information sharing objects are complex so it is necessary to establish customized information service structure. With the distributed characteristics of blockchain, the specific services for different objects can be layered to achieve the pertinence of services.

When the government information is written into the blockchain, the timestamping is automatically added as the existence proof of data flow, which is used to ensure that the information itself and its operation record cannot be falsified.

Blockchain will also introduce the factor of accountability of the users if any wrong information is been passed because blockchain ensure not digital footprint gets deleted.

Finally, the reliability degree of all nodes in the blockchain described in this paper is consistent, however the subsequent studies could analyse the realization of government information sharing mode under different degrees of trust from the perspective of reliability verification.

[2] is a survey based on Government Infrastructure Information. It provides a comprehensive review of various solutions adopted by governments of different countries around the world for effective use of Blockchain Technology in strengthening and securing information flow.

It defines Blockchain as an information system or a free, decentralized Internet server. It is like a virtual block and a database which can be shared across a multi-site, geography or institutional network. It is a consent-oriented, hierarchical data system, which provides all linked partners with a common public record and thus help build trust among the parties involved in virtual interactions, increase accountability and eliminate unnecessary intermediaries.

Some of the countries that used blockchain technology in their governance are Estonia, Israel, United Kingdom, South Korea, New Zealand etc. Most of the governments took help from national blockchain start-ups. Estonia migrated its public health records to Blockchain to monitor and prevent unauthorised access. Also, in its E-residency project, it provided people transnational identities using which citizens can vote securely and avail other government services. Israel has developed an IOT ecosystem in accumulation with Blockchain which aims to act as an electronic, chronologically modified, distributed and cryptographic data storage information structure. New Zealand used blockchain to access location, freshness, safety and quality of food products for revolutionising its agriculture sector. South Korea also used blockchain technology for voting system and also as a mechanism for ownership of property and settlement management. The United Kingdom is preparing to migrate its Payment and Banking Systems to Blockchain Technology. It believes that blockchain is the solution to its problem of complexity in tracking and controlling the use of subsidies. It is also open to all ideas, as Blockchains can be used in a number of areas, including government grants, that track cash and possibly improve taxpayers' offers.

Although some of the above-mentioned programs are very successful, most of them do not work on a scale and some are still in the planning phase. Simultaneously, a number of legal, ethical and technological hurdles are to be overcome so that blockchain and shared register technology in government can completely exploit its potential.

[3] provides introduction to a bare minimum prototype of a blockchain application for Government Fund Tracking using Hyperledger Composer and talks about the basics and applicability of blockchain in different domains. It proposes that using blockchain everyone can track all the amounts regarding when and where it is being utilized bringing in the much-needed transparency and thus reducing corruption.

The advantages of this system are: This blockchain model can provide transparency in all government transactions. So, there will be no discrepancies of any kind. Due to the decentralized ledger all the transactions can be verified and cannot be altered. The money that is released can be tracked, anyone and everyone can find out how the money is being used. As data is being stored across a peer-to-peer network, the blockchain removes a number of risks that come with data being held centrally. As the definition of blockchain states that every block has a cryptographic hash of the previous block, it confirms the integrity of the previous block all the way to the starting block.

The limitations we found in this model are: This model can be run on the Hyperledger Fabric on the cloud where the blockchain would be stored. Also, it poses privacy challenges. We have to be selective of the information about a transaction that is made available publicly. Moreover, the increase in complexity of the system is also there.

[4] presents research on Strong Supervision Algorithm Model Based on Blockchain in E-government. It proposes that Blockchain technology can be effectively used to solve the problem of unclear rights and responsibilities of government data resource through the non-tampered and traceable characteristics formed by the hash data structure between blocks .

Existing problems of blockchain application in e-government are:-

* The first step of building a government blockchain is to upload the data onto the chain. Because of the no-tamper characteristic of blockchain, the correctness of upload operation is important.
* The government data resources are divided into three categories as unconditional sharing data, conditional sharing data and non-sharing data based on Government Data-Data Classification Guide.

Based on the TRS algorithm, the report paper[4] proposes a strong supervision model to improve the traditional application scope of blockchain, and implement it by smart contract.

TRS ALGORITHM

TRS is a signature scheme that combines threshold characteristic with ring signature. The first threshold ring signature was proposed by Bresson, Stern and Szydlo in 2002, which is called the BSS threshold ring signature. In a (1, N) threshold ring signature scheme, the signature private key is kept by N members in a distributed form, and a valid threshold ring signature can only be generated if at least one member participates. That is, a member can execute a valid signature on behalf of the entire ring without the participation of other members, and the signature does not reveal the identity of the signer.

This paper [4] demonstrates the disadvantages of directly using the common blockchain in e-government. And secondly, based on the threshold ring signature (TRS), we propose a strong supervision algorithm called “L-sign”, which cleverly realizes strong government supervision on the basis of retaining the decentralization of blockchain.

Its advantages are as follows:

* we choose one application to verify the significance of strong regulation on the blockchain.
* The algorithm verification indicate that the strong supervision model can decrease the errors, increase the flexibility of blockchain so as to enhance the integration application of blockchain and e-government. sharing application of e-government and perfect it.

1. SOFTWARE REQUIREMENTS SPECIFICATIONS DOCUMENT

# **INTRODUCTION**

## **PURPOSE AND SCOPE**

Governments and public sector organizations can leverage blockchain technology to move away from siloed and inefficient centralized systems. Current systems are inherently insecure and costly, while blockchain networks offer more secure, agile, and cost-effective structures.

We intend to automate the monetary distribution using blockchain. At each level of distribution, transactions will be bound in digital blocks which will be dependent on their parent block for their existence. Every person in the government hierarchy will have access to the data of these transactions and thus providing transparency in the system.

According to the Income Tax Department of India, only about 1% of the total population pays service tax and they pay tax using either of the given two means- Digitally or through Cheques or Challans at bank. Banks then also make the further transactions digitally. As the taxes are already being paid digitally, so it won't be very difficult migrating to another digital environment. Hence, there is a scope of actually implementing this idea practically.

## **ABBREVIATIONS**

|  |  |
| --- | --- |
| **Abbreviations** | **Full Form** |
| js | javascript |
| HL | HyperLedger |
| gov | government |
| SSL | Secure Sockets Layer |
|  |  |

## **INTENDED AUDIENCE AND READING SUGGESTIONS**

The intended readers of the document would be-

* Developers
* Users: Government Officials, Tax Payers, Contractors, etc.

## **REFERENCES**

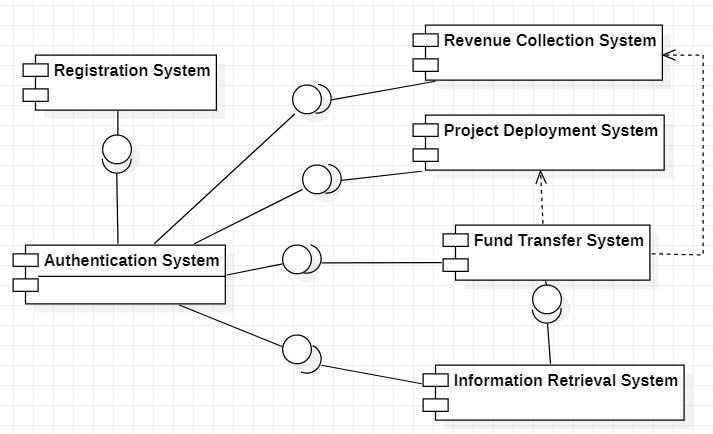
1. <https://ieeexplore.ieee.org/document/8964638>
2. <https://ieeexplore.ieee.org/document/9203152>
3. <https://ieeexplore.ieee.org/document/8769200>
4. <https://ieeexplore.ieee.org/document/9141657>

# **OVERALL DESCRIPTION**

## **PRODUCT PERSPECTIVE**

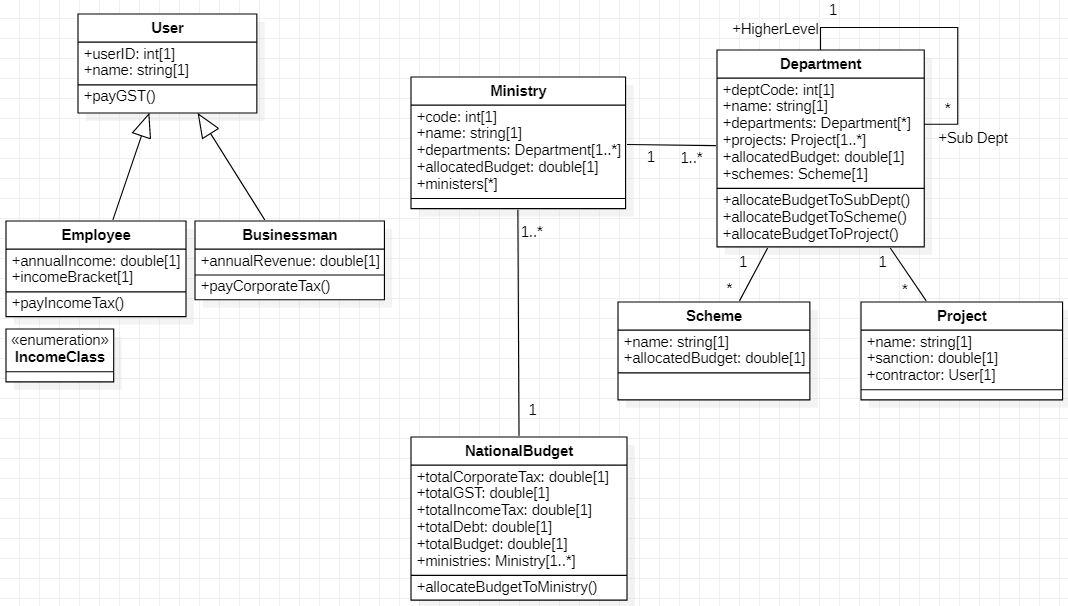
Major components of the system:

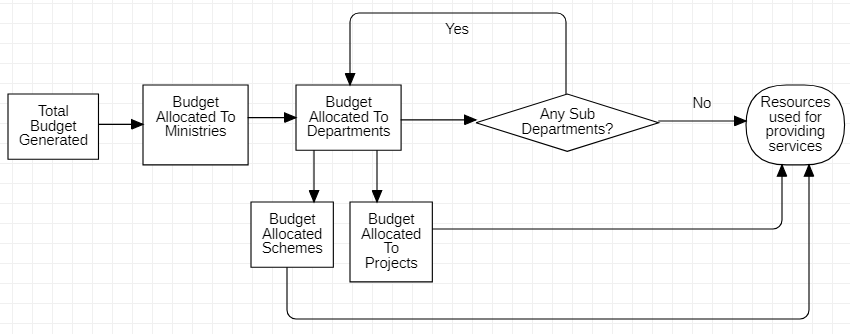
* Registration System: This component will be used to register new users to the system.
* Authentication System: This component will be used to verify the identity of the person logging into the system.
* Revenue Collection System: The component to collect corporate taxes in the form of cryptocurrency.
* Project Deployment System: The component to deploy new projects on different levels of the system as per the requests generated by the concerned departments.
* Funds Transfer System: This component involves methods to make transactions of funds from one level to next. It involves adding a new block of transaction to the blockchain in every connected computer in the decentralised system.
* Information Retrieval System: This component is responsible for adding transparency to the whole model. It will answer different queries made on different hierarchical levels. As blockchain is integrating consistency in the system so any flaw in the transactional details will be easily detected.



## **PRODUCT FUNCTIONS**

* A User can Pay Taxes (Income Tax, Corporate Tax, GST, etc), which get recorded in Blockchain as Transactions.
* Total Budget is Generated By summing up funds from various resources such as taxes, non-tax revenues, union excise duties, borrowings and liabilities, etc.
* The Budget is then distributed between various Ministries of the gov. like Defence, Home Affairs, Railways, Agriculture, Health etc.
* Each Ministry may have different departments, the budget is then further divided into the departments.
* The departments further may have sub departments and lower levels. Each department will sanction money grants to various projects/departments under its control as per the request.
* Each Department will get its projects approved from top level authorities.
* Each transaction of allocation of budget is also recorded as a new block in the blockchain.

CLASS DIAGRAM:

FLOW CHART:

## **USER CLASSES AND CHARACTERISTICS**

The various user classes that will use this product are:

* Tax Payers: Users can pay their taxes through this platform and also query where and how the governments funds are being used, hence making the bureaucratic institution transparent to the citizens of the country.
* Government officials: Characteristics of officials depend on their department.
  + Central Authority: These officials collectively decide which projects from the lower-level departments requested are required and valid to approved. They vote to decide if a certain project can be deployed or not.
  + Project/Department: The officials can request to deploy various sub-projects in their departments. Officials in a sub-project can ask for money grants for their working occasionally when required from their higher-level department/project. Officials in higher-level project vote to decide if the money grants requested are actually required and genuine and approve them to be issued.
  + Tax Collection: Officials verify and add new tax payers and regulate various tax brackets and tax cycles.

All users should be familiar with web technology. However, users should have a good understanding of the tasks, activities, and artifacts of either process in which they may be interested.

## **OPERATING ENVIRONMENT**

The server-side components will operate on a cloud-based platform like Google Cloud Platform and Hyperledger to host the blockchain systems application.

The client-side components of the software system must operate within common web browser environments using SSL / Transport Layer Security (TLS) cryptographic protocols at a minimum encryption level of 128 bits.

For the purpose of cryptography, bcrypt library will be used primarily.

The main Tech Stack involved is for application development are:

* Node.js
* Blockchain( Powered by js)
* HTML / CSS

For API deployment following platforms are considered.

* Firebase
* Heroku

Other than this basic model, mobile applications can also be provided to the users of different levels.

## **DESIGN AND IMPLEMENTATION CONSTRAINTS**

* It is difficult to gather detailed knowledge about the internal distribution structure of the gov. and some aspects may even be confidential, therefore, we can only implement a high-level view of the monetary distribution system.
* The actual budget is collected from a variety of different sources, it is very difficult to understand in depth all those financial sources like various divisions of taxes, debt from other governments. Therefore, only the most common and basic taxes will be included.
* If there is a need to roll back the transactions of already allocated funds due to fluctuations in GDP, it cannot be done as blockchain transactions are not reversible, therefore no administrator can fix any real errors. We will have to generate new transactions.

## **USER DOCUMENTATION**

* Every new user will be given an introductory tour of the basic functionalities of the application on very first login.
* We will provide a list of FAQs to solve some common queries.
* An online documentation will be provided to look up for the use of any functionality of the application.

## **ASSUMPTIONS AND DEPENDENCIES**

ASSUMPTIONS-

* The Monetary Distribution Model structure, as shown in the Class Diagram is a high-level abstraction of the actual complex structure of the Distribution System, assumed by us based on our understanding.
* It is assumed that there are only one kind of tax payers and one kind of tax, which is applied yearly on the annual income of the tax payers as per the tax bracket he/she falls in.

DEPENDENCIES-

* We will rely on platforms like Firebase Authentication for making custom ID templates for the registration.

# **EXTERNAL INTERFACE REQUIREMENTS**

## **USER INTERFACES**

* The inputs will be entered via web control like checkbox, text box, etc.
* Every page will have the disclosure text and font will be set such that they are compatible with different browsers.
* Navigation and acceptance will be handled with buttons.

## **HARDWARE INTERFACES**

In the initial phases of our project, websites will be the standard platform for accessing the product. But it can be completely scalable over mobile devices as well.

For the developer, different hardware interaction can be  accomplished using instances of different machines over platforms like GCP and AWS. Everything will be requirement specific and can scale or shrink with time.

## **SOFTWARE INTERFACES**

* The Authentication system shall communicate with the Registration system to confirm the credibility of user login.
* Information Retrieval system shall communicate with Funds transfer system to answer any query made by the users(Contractors or Government Officials).
* The Revenue collection system shall communicate with the tax collecting authorities and banking machinery(RBI) for timely money intake.
* Once the funds start moving within the government machinery, different levels of the blockchain shall communicate with the parent node for making a new entry.

The underlying software functions are bound to use system call for the interaction among different functionalities. There will be a scenario when network call will also be executed because client side and server-side software are independent entities.

## **COMMUNICATION INTERFACES**

The system will use TCP IP protocol for communication and HTTP protocol for websites. User form data will be transferred using HTTP-POST method and search data will be transferred using HTTP-GET method. Password data will be encrypted. Any query to the Hyperledger will be handled through the API’s.

In the whole of this communication process JSON format will be used to exchange the data.

1. USE CASE DIAGRAM

