
# Department of Information Technology

A.P. Shah Institute of Technology

G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615

UNIVERSITY OF MUMBAI

Academic Year 2019-2020

A Project Report on

# Expeditious Banking using Blockchain Technology

Submitted in partial fulfillment of the degree of
Bachelor of Engineering(Sem-7)

in

**INFORMATION TECHNOLOGY**

By
Varsha Naik(16104054)
Riya Pejawar(16104040)
Rishabh Singh(14104017)

Under the Guidance of
Prof. Anagha Aher
Prof. Sneha Kanchan

# 1.Project Conception and Initiation

# 1.1 Abstract


- Blockchain is growing as a potentially Out of line force capable of changing the financial services industry by making the fund transfer immediate, cheaper and more secure.
- Current existing system is not secure enough to give 100% fraud protection because of more manual work and lack of security of data. Blockchain is nothing but a chain made of blocks (nodes).These process nodes do the all major work. These blocks are connected to each other using cryptography.
- This system will be more expeditious, more efficient, and has user affectional interfaces in the banking and has zero probability of losing data while processing of the user data.
- In integration to enabling trade, block chain is larceny-and tamper-resistant model, it eliminates errors and the duplication, blockchain is ideal for reserving the data in blocks and using a tamper-proof hash format, so the data can be securely stored by bank and make the current existing system much more secure and faster.

# 1.2 Objectives

- To decentralize the entire banking scenarios.
- To make sure no one can manipulate or bypass the system.
- To ensure all the rules laid down by RBI are strictly abided to and none supersided.
- To protect the inter- block chain data from foreign entities through encryption techniques and checksum generation .

# 1.3 Literature Review

- **An Overview of Block chain Technology: Architecture, Consensus, and Future Trends:**

Block-chain serves as an immutable ledger which allows transactions take place in a decentralized manner. However, there are still many challenges of block-chain technology such as scalability and security. This paper presents a comprehensive overview on block-chain technology. We provide an overview of block-chain architecture firstly and compare some typical consensus algorithms used in different block-chains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for block-chain.

ADVANTAGE: **Hashing and PKI Cryptography.**

DISADVANTAGE: **Only systems in the network are secured.**

# 1.3 Literature Review

- **Building a block cipher mode of operation with feedback keys**:

In this paper, we propose two block cipher modes of operation named the Key Stream Protection Chain mode (KSPC) and Output Dual Chaining mode (ODC), which differ from other existing BCMOs , the cipher text block and in the ODC, the block cipher encryption unit's output are fed back to the encryption system to be one of the inputs of the next block ciphering. We also evaluate three existing BCMOs, including the Cipher Block Chaining mode (CBC), the Propagating Cipher Block Chaining mode (PCBC) and the Output Feedback mode (OFB), and discuss the security of the these modes when they face chosen-plaintext attacks.

ADVANTAGE:**Block Cipher Encryption**
DISADVANTAGE: **If keys are available, its easily hacked.**

# 1.3 Literature Review

- **A small JAVA Application for Learning Blockchain:**

This paper introduces a small Java application named ChainTutor for learning basic Blockchain concepts. With the Java Application used in this paper, users can experiment with key Blockchain concepts through graphical user interface. The Java application is intended to be used in classroom environment by instructors when they teach introductory blockchain courses.

ADVANTAGE: **Java Microservices**.

DISADVANTAGE: **Logic is pre- defined, cannot be changed.**

# 1.4 Problem Definition

- To build an efficient and secure banking architecture using block-chain technology.
- Current banking architecture is largely centralised and therefore vulnerable to loan defaults and frauds like the PNB scam, Videocon case , Kingfisher scam and many more.
- Banking all over the world has adopted block chain technologies and it is the need of the hour for regulation and avoidance of such scams.
- Thus, we are using block chain technology for the decentralized working of banks and the complete removal of authoritarian interception.
- Software used: Java micro services, PKI , MAC hashing , Checksum generator for security module
- Hardware used: Laptop, cable, USB, SQL database, network support.

# 1.5 Scope

- To create an expeditious banking system .
- To ensure a decentralized banking transaction for NEFT using block-chain technology.
- Create a banking prototype for user interface for connecting the user to the backend processing.
- To ensure protection of data in transit i.e. inter-block communication by hashing and cryptographic algorithm.
- To ensure blocks are not bypassed by ensuring checksum matches by the majority in the pool of blocks.

# 1.6 Technology stack

- Software Requirement

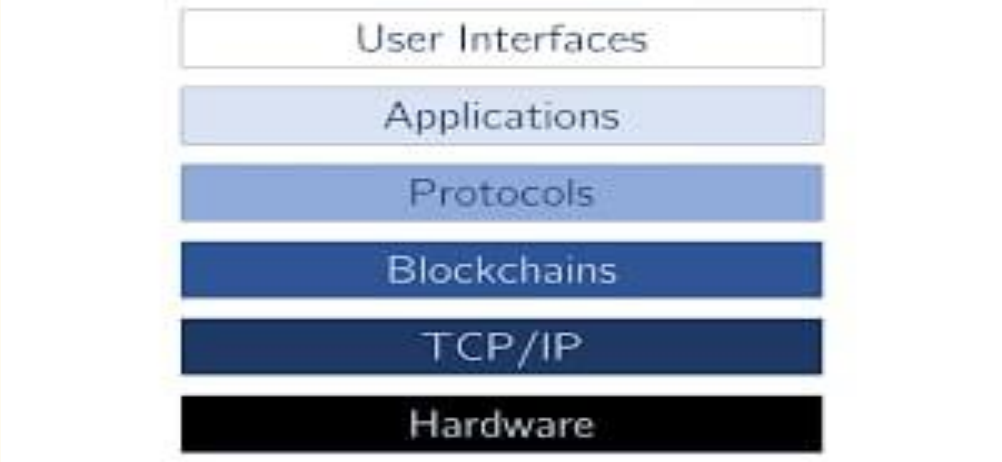
| | |
|---|---|
| Operating System | Windows xp or later |
| Web Server | Apache Tomcat |
| Programming Languages | HTML5, CSS3, java ,SQL, JavaScript. |
| Database Technology | MySQL |
| Interface Application | Web Application |
| Browser Support | Any |

# 1.6 Technology stack

- Hardware Requirement

| | |
|---|---|
| **PROCESSOR** | Dual core or more |
| **RAM** | 2GB |
| **Hard Disk** | 100MB |
| **Internet** | 2MBPS |

# 1.6 Technology stack



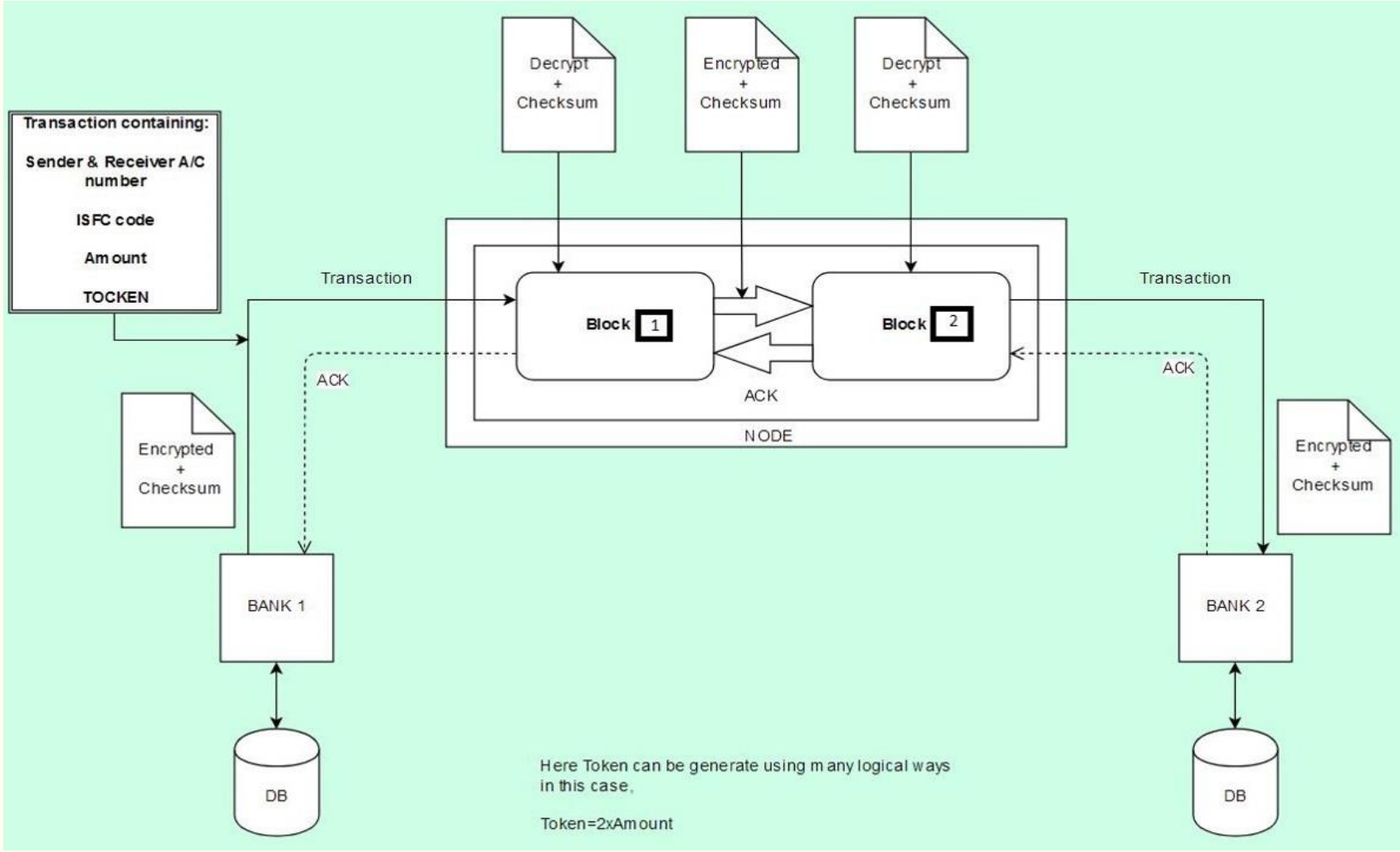
# 1.7 Benefits for environment & Society

- Our project is an efficient solution for bypassing human intervention and control in banking sector to make it reliable and secure.
- The project will ensure decentralized transfer of funds.
- Frauds and huge loans sanction can be done away with our perception of a solution using Blockchain which makes it free of manual intervention.

# 2. Project Design

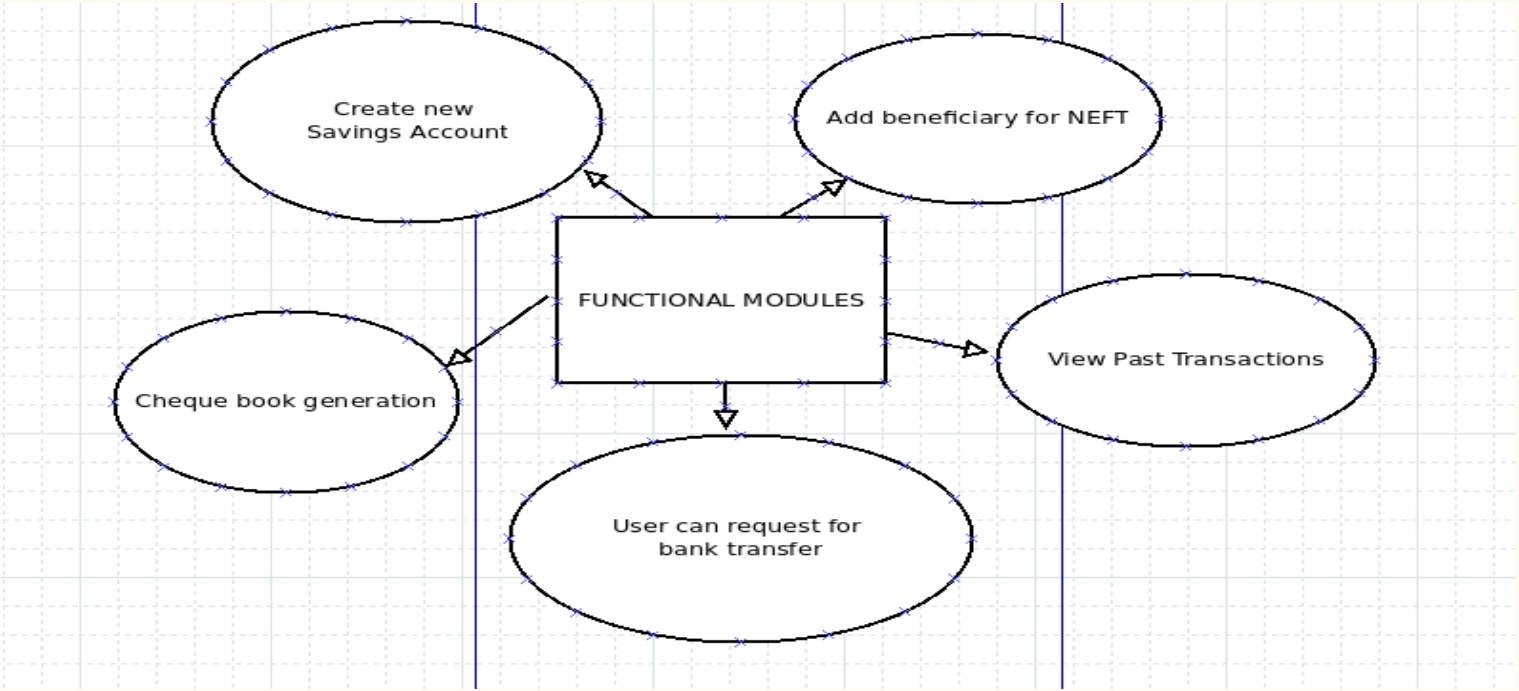
# 2.1 Proposed System

- The web application will help the bank users to perform the banking transaction more securely and with faster response by eliminating the third parties and the concept of blockchain technology is used which is very power full as compare to other modern world technology.
- The system includes two main modules User, Admin.
- User module contains sub-modules such as money transfer, OTP generation, My statement, Add beneficiary.
- Admin module has viewing of all of the user request and add branch.


Transaction containing:
Sender & Receiver A/C number
ISFC code
Amount
TOCKEN
Decrypt + Checksum
Encrypted + Checksum
Decrypt + Checksum
Transaction
Block 1
Block 2
ACK
ACK
NODE
Transaction
ACK
Encrypted + Checksum
Encrypted + Checksum
BANK 1
BANK 2
DB
DB
Here Token can be generate using many logical ways in this case,
Token=2xAmount

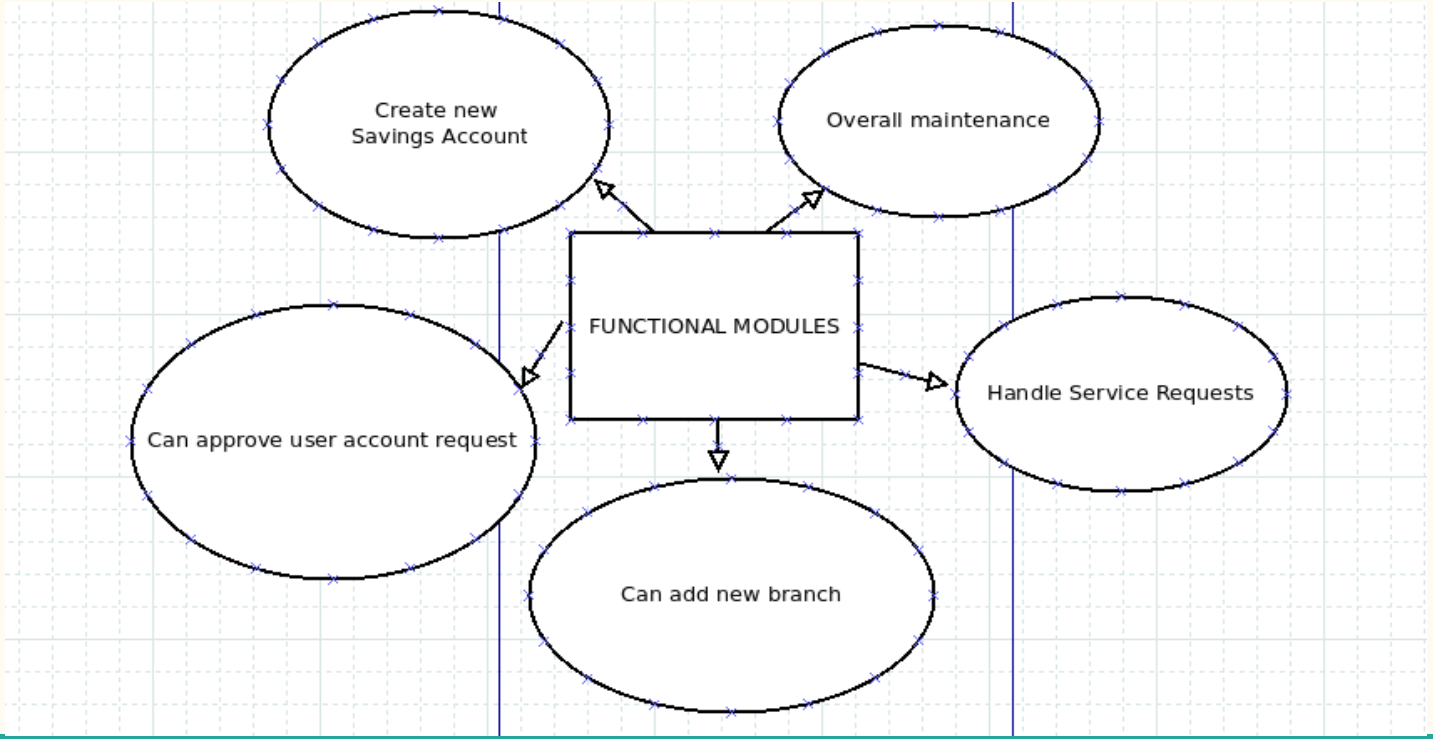
# 2.2 Design(Flow Of Modules)

- User Module



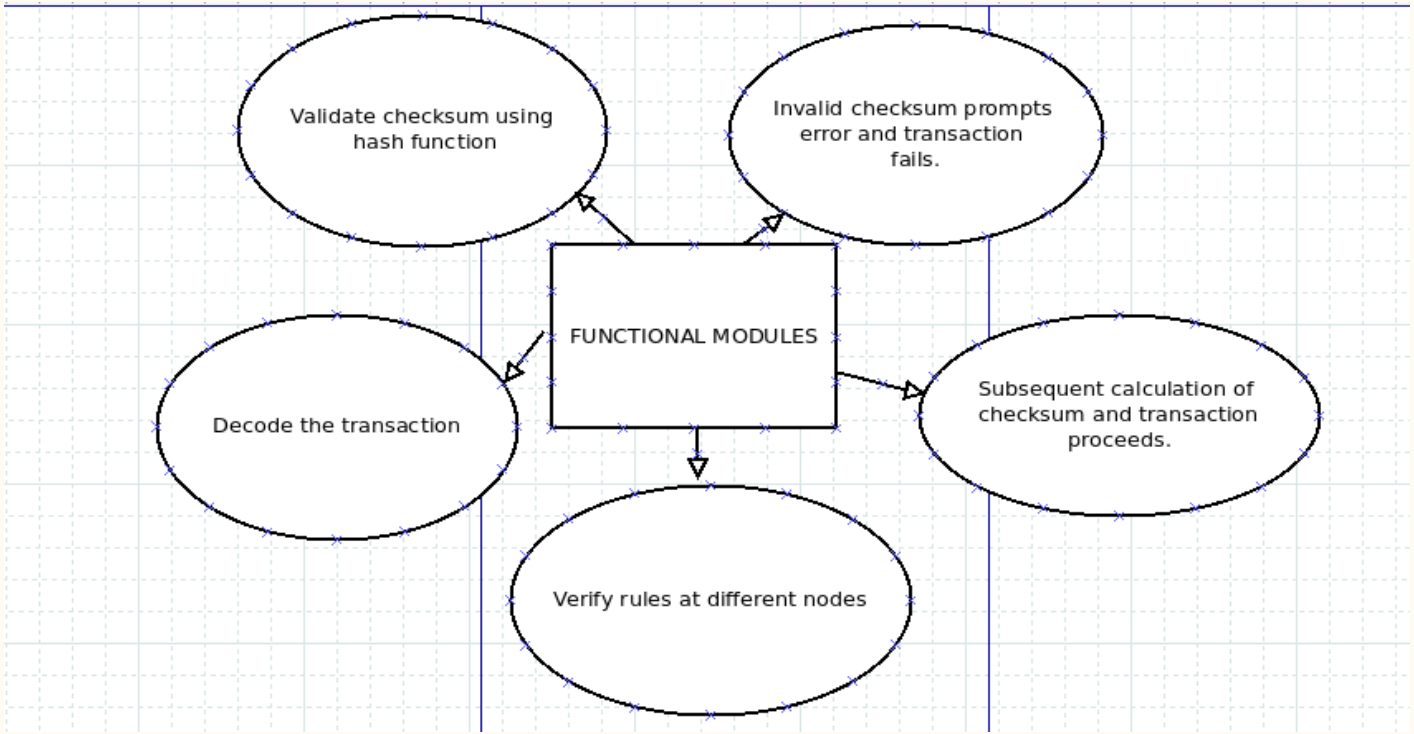
# 2.2 Design(Flow Of Modules)

- Admin Module



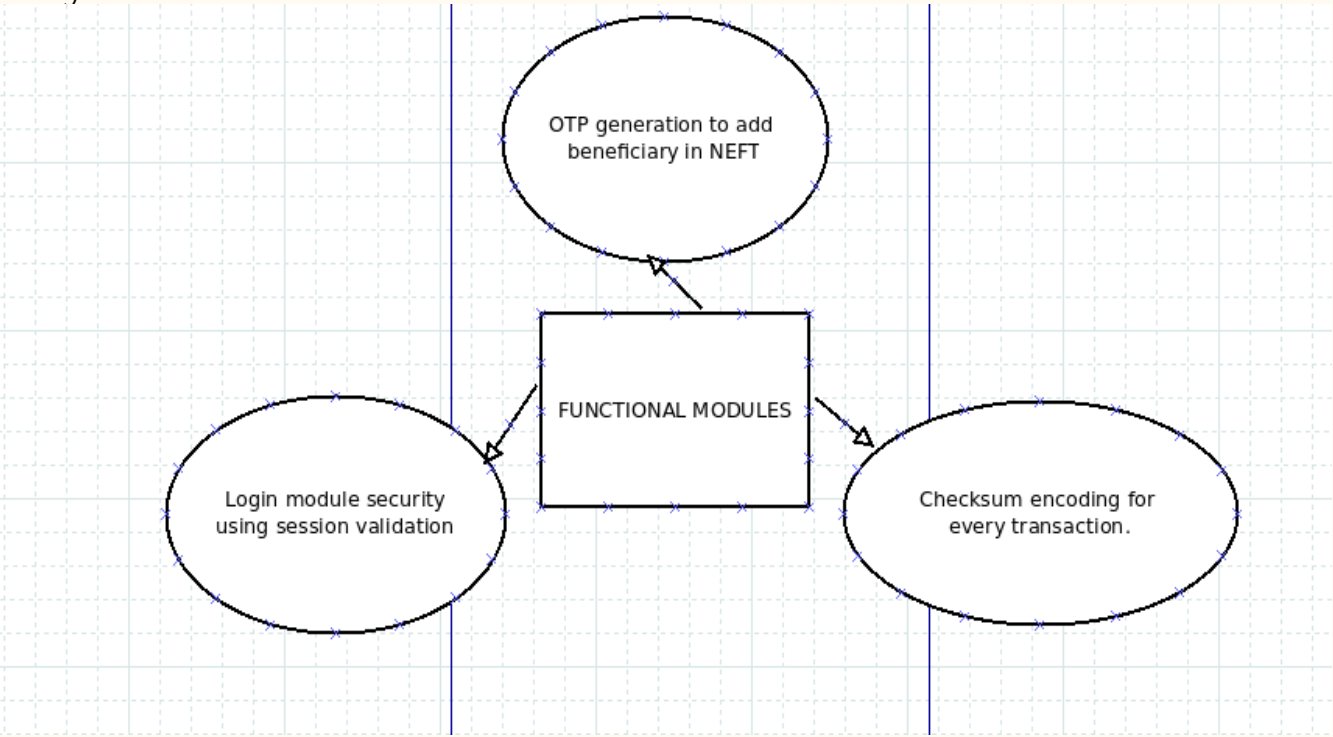
# 2.2 Design(Flow Of Modules)

- Block-chain Module

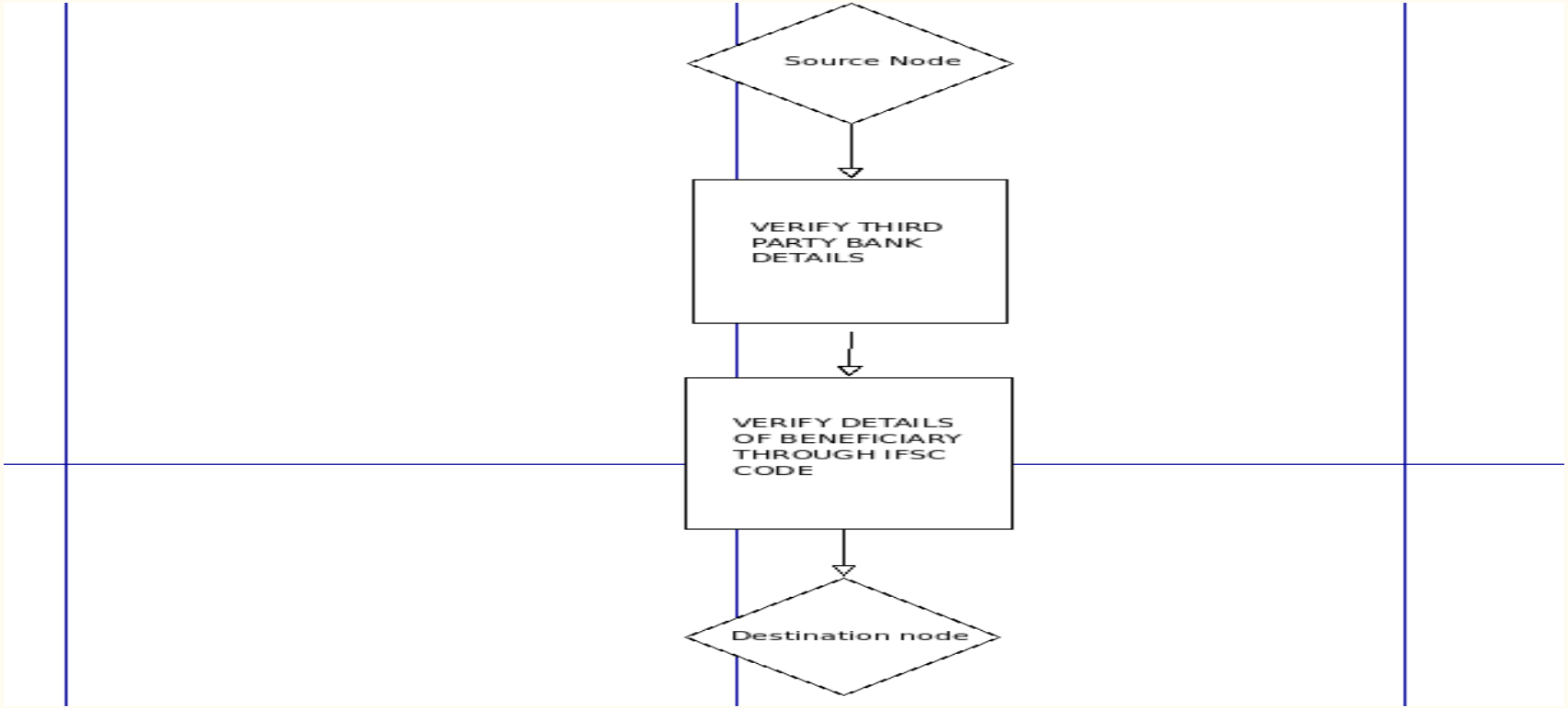


# 2.2 Design(Flow Of Modules)

- Security Module

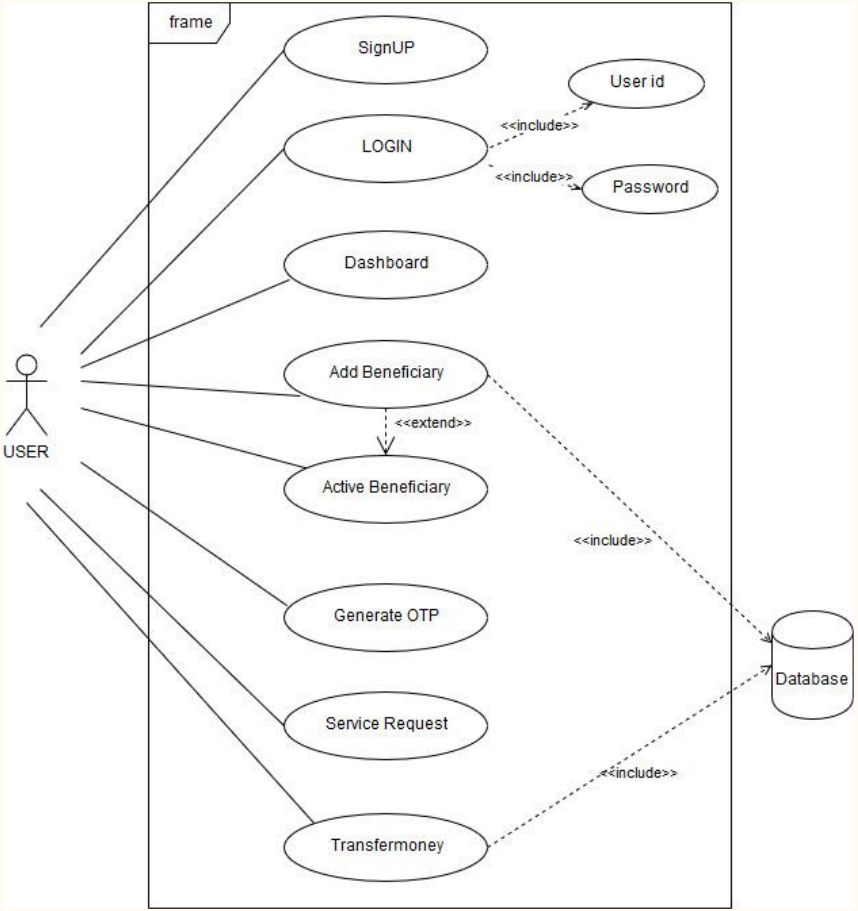


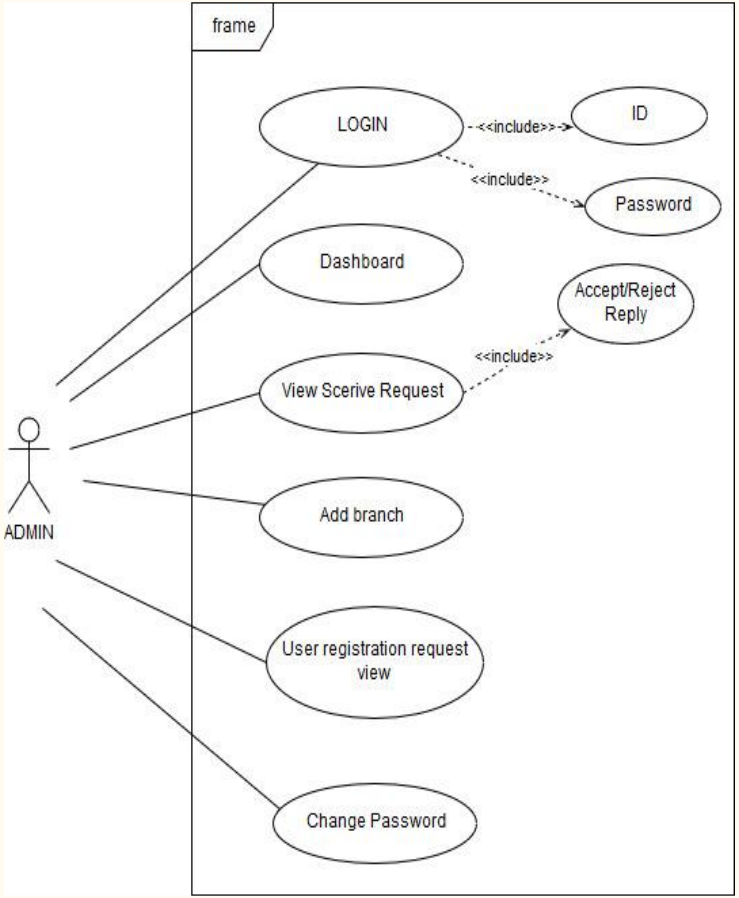
# 2.2 Design(Flow Of Modules)



# 2.3 Description Of Use Case

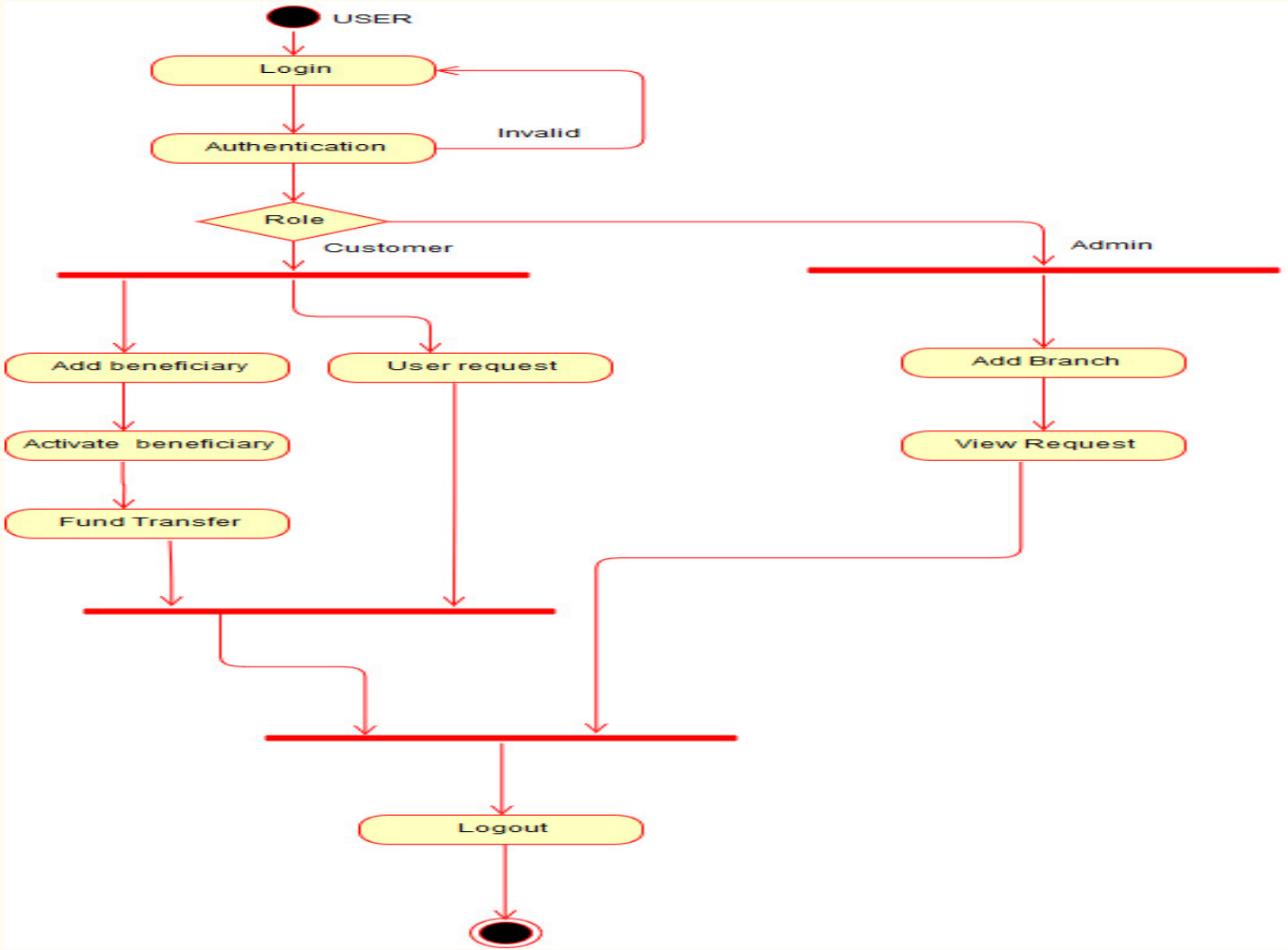
It shows the user’si nteraction with the systems. The purpose of a use case diagram in Unified Modeling Language (UML) is to demonstrate the different ways that a user might interact with a system. Use case diagrams are valuable for visualizing the functional requirements of a system that will translate into design choices and development priorities.They also help identify any internal or external factors that may influence the system and should be taken into consideration. In first use case diagram there are two main components one is actor which is user and and database. It depicts the interactions between the various actors used in this system. All these interactions between actors and system is done in the cloud environment. There are various usecases involved in this system such as register, addbeneficiary, activate beneficiary, view my statements, generate one time password etc. The other use case diagram has only one actor which is admin. Admin also has various use cases such as add branch,view all user requests and approve them.


frame
SignUP
User id
LOGIN
<<include>>
<<include>>
Password
Dashboard
Add Beneficiary
<<extend>>
Active Beneficiary
<<include>>
Generate OTP
Service Request
Transfermoney
<<include>>
Database
USER


frame
LOGIN
<<include>>
ID
<<include>>
Password
Dashboard
Accept/Reject Reply
<<include>>
View Scerive Request
Add branch
User registration request view
Change Password
ADMIN

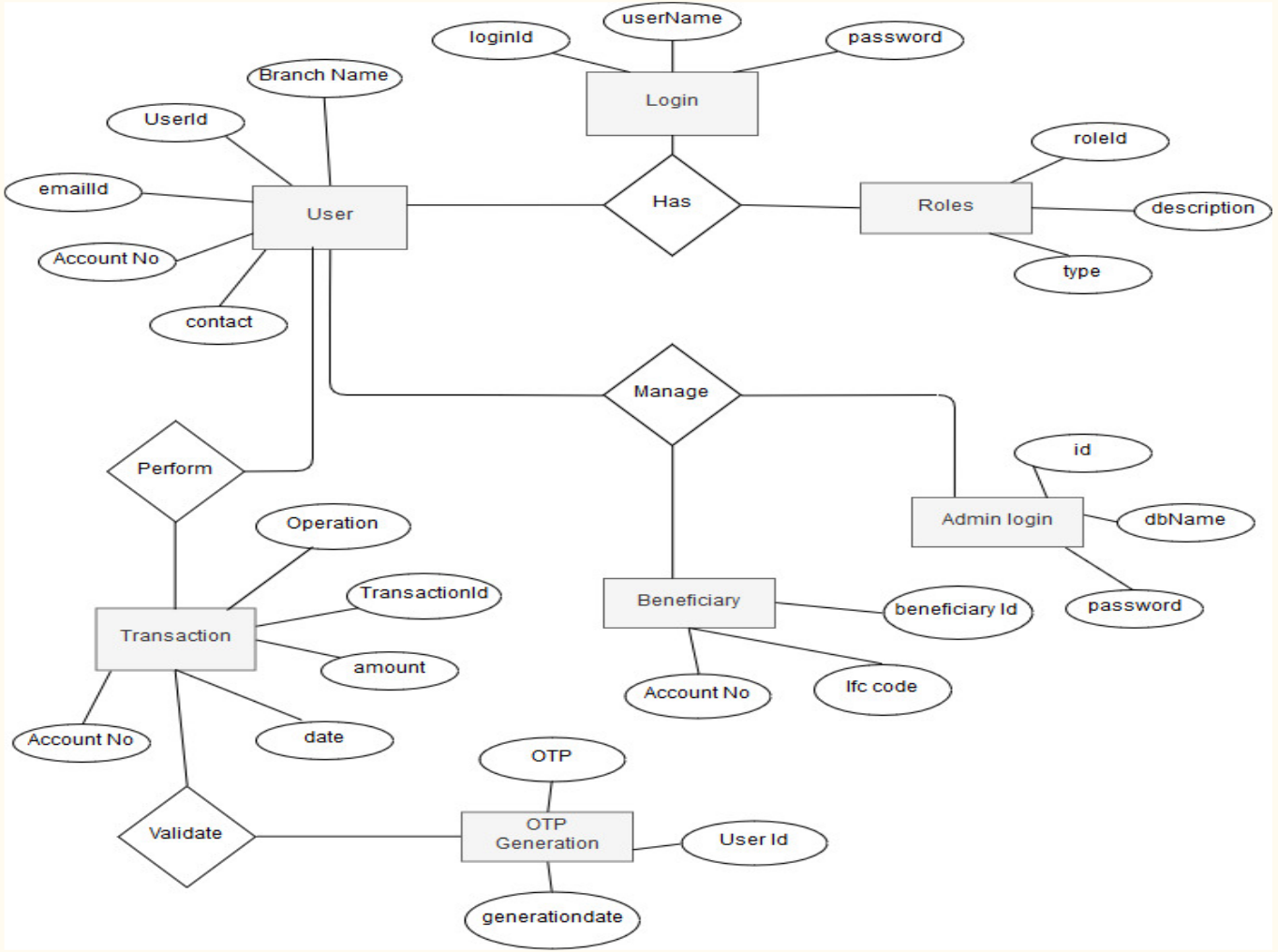
# 2.4 Activity diagram

Activity diagram is a flowchart to represent the flow from one activity to another activity. The basic purposes of activity diagrams is similar to other four diagrams. Activity diagrams are not exactly flowcharts as they have some additional capabilities. It captures the dynamic behavior of the system. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. It captures the dynamic behavior of the system. Activity diagrams are used for visualizing the system.

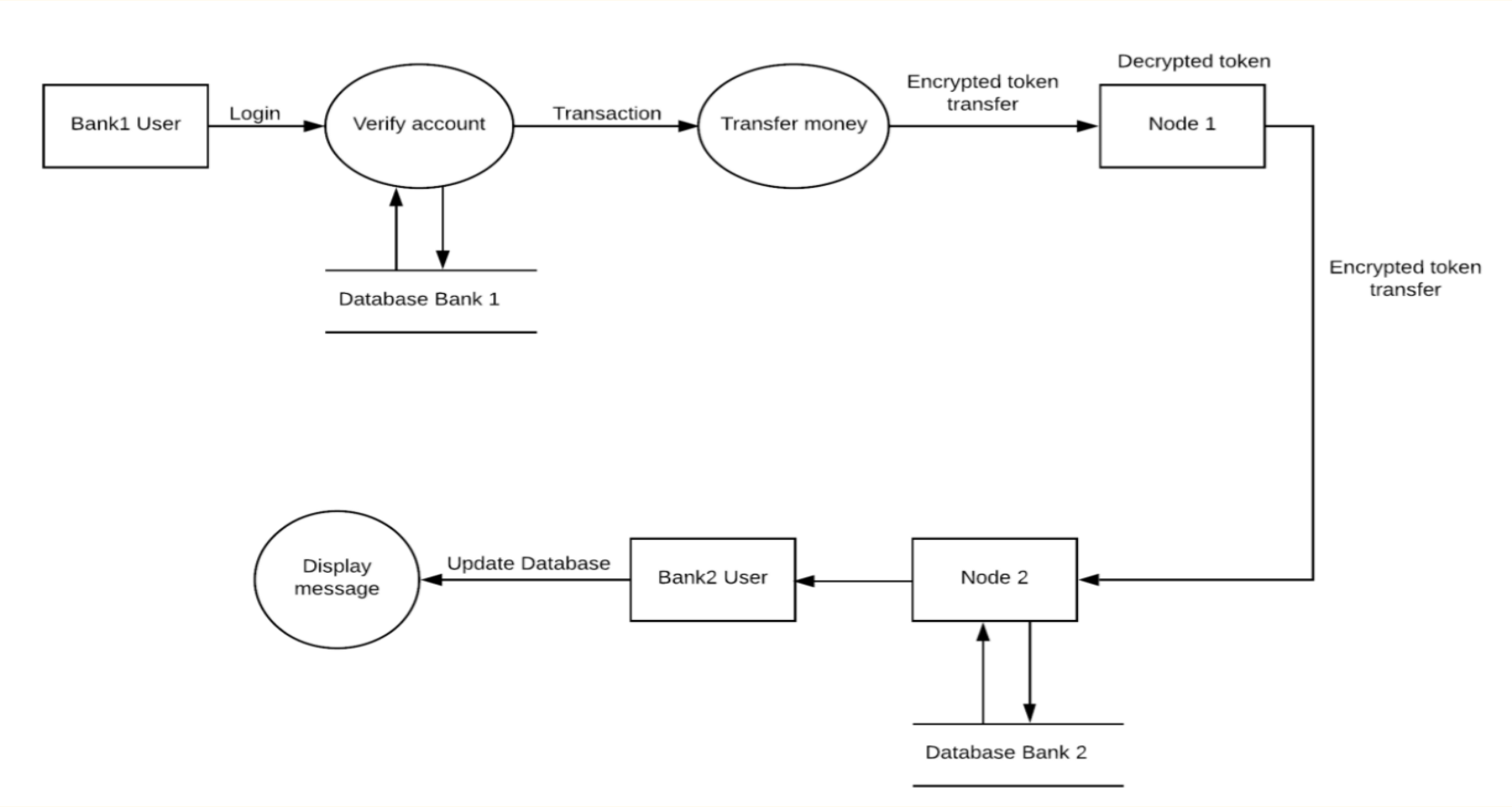

USER
Login
Authentication
Invalid
Role
Customer
Admin
Add beneficiary
User request
Activate beneficiary
Fund Transfer
Add Branch
View Request
Logout

# 2.5 Entity Relationship Model

Here, the entities are:- User, Login, Roles, Transaction, Beneficiary, Admin, Otp generation. First admin is major entity as the admin controls banking activities. Admin logins using the credentials which are already assigned to admin. These credentials has predefined roles and according to these assigned roles it’s determined that visitor is admin or user. These roles have attributes such as id,role description,type ie. user or admin. Admin also have attributes such as name,id,contact.Now User logins using his credentials roles are assigned to them. So, user has roles. User has various attributes such as name,account number, id, contact. Now user manages beneficiary ie. add/remove and activate beneficiary. Beneficiary has various attributes such as name,his branch ISFC code,account number. Now user has relationship with transaction of performing it so user perform transaction.


userName
loginId
password
Login
Branch Name
UserId
emailId
User
Has
Roles
roleId
description
type
Account No
contact
Manage
Perform
id
Admin login
dbName
password
Operation
TransactionId
Transaction
amount
Beneficiary
beneficiary Id
Account No
Ifc code
Account No
date
OTP
Validate
OTP Generation
User Id
generationdate

# Data Flow Model



# 2.6 Module-1:BANK 1

**Bank User**

- The application consists of the User interface with all the required links and buttons for navigating inside banking application.
- For sign up user has to provide the personal details like Name, email, PAN.
- After sign up the user will receive the mail containing the details like login id, login password.
- Whenever user wants to do the transaction user has to enter transaction password theuser can proceed with transaction.

**Bank Admin**

- This part of an application also consists of the User interface with all the required links and buttons for navigating inside banking application.
- Whenever new user register himself as new customer this request is received by admin, once admin approve this user gets mail of acceptance along with credentials in it.
- The admin has the ability to accept or reject the service requests of users, he can also add the new branches of his bank into the system.

# **Module-2 :** Processing NODE 1

- A node is a device on a blockchain network, that is in essence the foundation of the technology, allowing it to function and survive.
- Nodes are distributed across a widespread network and carry out a variety of tasks.
- The blocks of data are stored on nodes (compare it to small servers). Nodes can be any kind of device (mostly computers, laptops or even bigger servers). Nodes form the infrastructure of a blockchain.
- All nodes on a blockchain are connected to each otherThis unit of an application is one of the main processing component of the system which runs in background without having any user interface.
- The whole transaction process is divided into two different blocks.
- NODE 1 is first block and the responsibility of it is validating the sender bank and the user by decrypting the token encrypted from the requested transaction.
- Another responsibility is again encrypting the decrypted token to send it securely on network to next processing unit NODE 2. If this unit fails the system will not work.

# **Module-3 :** Processing NODE 2

- The nodes (blocks) are connected to each other forming a chain of blocks. The NODE 2 is the second processing unit of entire banking system which runs in background.
- Transaction packet encrypted by NODE 1 is received by NODE 2.
- Now NODE 2 decrypt this package then NODE 2 validates the receiver’s bank, receiver’s name also because money should not get sent to other user by mistakenly and Indian Financial System Code(ISFC).
- After that updating the receiver’s bank database and giving the acknowledgement for the same to sending bank user. Nodes follows consensus algorithm.

# Module-4 : BANK 2

**Bank User**

- The application consists of the User interface with all the required links and buttons for navigating inside banking application.
- For sign up user has to provide the personal details like Name, email, PAN.
- After sign up the user will receive the mail containing the details like login id, login password.
- Whenever user wants to do the transaction user has to enter transaction password theuser can proceed with transaction.

**Bank Admin**

- This part of an application also consists of the User interface with all the required links and buttons for navigating inside banking application.
- Whenever new user register himself as new customer this request is received by admin, once admin approve this user gets mail of acceptance along with credentials in it.
- The admin has the ability to accept or reject the service requests of users, he can also add the new branches of his bank into the system.

# 2.7 References


- An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3

- Building a block cipher mode of operation with feedback keys Yi-Li Huang, Fang-Yie Leu, Jung-Chun Liu, Jing-Hao Yang, Chih-Wei Yu, Cheng-Chung Chu, Chao-Tung Yang Department of Computer Science, TungHai University, Taichung ,Taiwan

- A Small Java Application for Learning Blockchain Xing Liu Dept. of Computer Science and Information Technology Kwantlen Polytechnic University Surrey, Canada

# 3.Planning for next semester
—

# Planning

- To finish with NODE-2 development with all functional requirements satisfied and all classes working properly.
- To finish with Bank 2 UI which will include the Admin dashboard and it’s functional aspects.
- To link all four modules within themselves with smooth and non-erroneous interfaces .
- To achieve the end result of an expeditious banking transaction using block chain.
- Present with a full working project in all respects.

# Thank You