Low Level Design

Blockchain Enabled KYC processes for Financial Institutions

Revision Number: 1.0

Last date of Revision: 25/11/2021

Team Members

Jitendra Sharma	B2020022
Nishita Mehta	B2020032
Shalini Singh	B2020050
Siddharth Kumar Singh	B2020054
Sudharshanam S	B2020057

Document Version Control

Date Issued	Version	Description	Author

Table of Contents

1 Introduction

1.1 What is a low level design document?

The purpose of a low level document is to explain the granular level working of the Blockchian based KYC verification processing. The low level design document contains all the modules that will be used while programming. The document contains the diagram of the flow of the program as well as the description of each module. This facilitates the programmer to have a clear understanding of the modules they are working for.

1.2 Scope

The document necessarily covers the program flow and the sequences in which the modules function. This process can be used for designing the data structures, for software architecture and the source code. This document does not include the various modules that can be further linked to provide additional functionalities.

2 Architecture

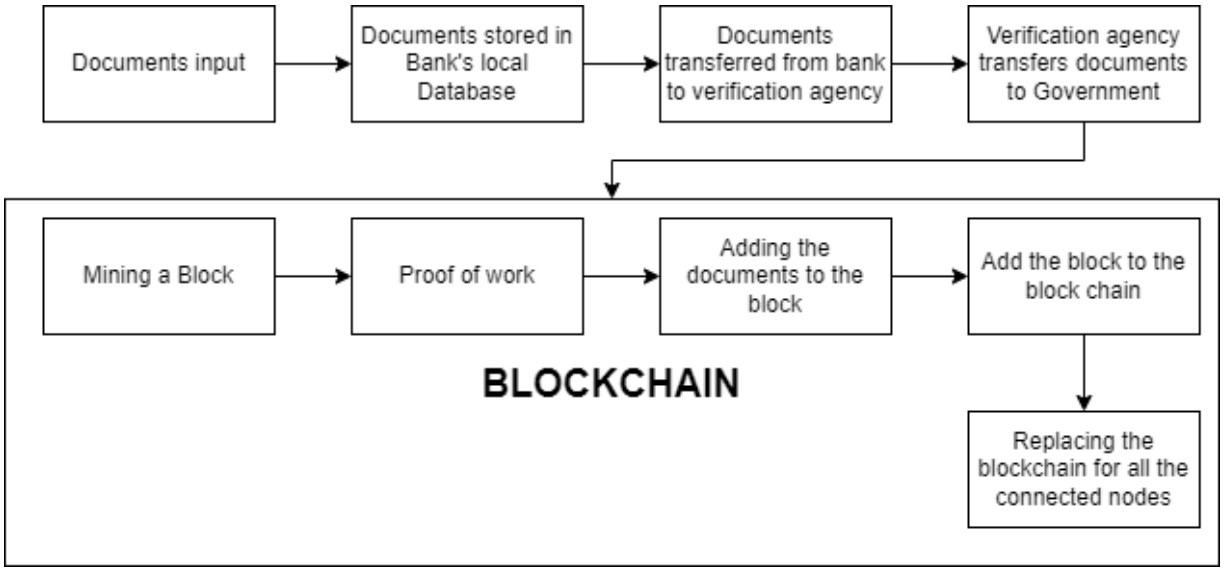

Figure 1: Program Flow Architecture

3 Architecture Description

3.1 Documents Input

The first step is for the customers to upload the KYC documents to the bank's online portal. The customer does this document upload only to the first bank the customer is going to. Which means that he/she does not have any bank accounts previously or had done any KYC verification previously.

3.2 Storage in local database

The uploaded files get stored in the bank's local database. The banks maintain these databases only for the temporary storage of the customer's files.

3.3 Documents transferred to verification agency

In this stage, the bank transfers the documents to an external verification agency. The external verification agency will perform the physical verification of the customer, their identity and their other details.

3.4 Agency to the government

Once the external verification agency completes the verification, they authenticate and certify the verification done and transfer the verified documents to the government.

3.5 Mining a block

It is the process of finding a nonce which satisfies the HASH restrictions. In this architecture, the government is assumed to be the one's building and maintaining the blockchain. Once the documents are received by the government, they mine a block with the requisites.

3.6 Proof of Work

While mining a block, once the hashkey is generated, the hashkey is verified for the predetermined sequence. If the condition is satisfied, the proof of work is complete. If not, the hashkey is again generated.

Algorithm for Hashing: SHA – 512

SHA 512 has 128 characters as compared to SHA 256 with 64 characters.

The reason for choosing SHA-512:

- It is faster than SHA-256 on 64-bit machines is that has 37.5% less rounds per byte (80 rounds operating on 128 byte blocks) compared to SHA- 256 (64 rounds operating on 64 byte blocks)
- It is more secure than SHA 256

3.7 Adding data to block

Once the proof of work is completed successfully, the verified data documents are added to the block.

3.8 Adding to the blockchain

Once the block is created successfully, the block will be added by the government to the blockchain.

3.9 Broadcasting the updated blockchain

The updated blockchain is now being broadcast to all the nodes (banks) in the network. This is done by replacing the blockchain of all the nodes with the new blockchain along with the added block.

If a new bank wants to get integrated to the blockchain, then an add node module is used to add the node to the blockchain network.