**A close up of a logo

Description automatically generated**

**ASR Belize Project**

Blockchain Design Document

Phase 1

**Table of Contents**

[1.0 Introduction 3](#_Toc100519049)

[1.1 Purpose 3](#_Toc100519050)

[1.2 Scope 3](#_Toc100519051)

[1.3 Version History 3](#_Toc100519052)

[2.0 Environment Details 3](#_Toc100519053)

[3.0 Proposed Design 4](#_Toc100519054)

[3.1 Assumptions 4](#_Toc100519055)

[3.1 Network structure: 4](#_Toc100519056)

[3.2 Smart contracts 5](#_Toc100519057)

[3.2.1 User Handling 6](#_Toc100519058)

[3.2.2 Loan application request 7](#_Toc100519059)

# 

# 1.0 Introduction

This document is designed to be a reference for the blockchain solution. It is a supplementary for the existing application design document. This document should be read by an individual with a technical background and basic understanding in blockchain technology.

The purpose of this software design document is to provide an insight into the structure and design of each component required for this project.

## Purpose

The purpose of this document is to define the architecture design for the blockchain network,

and define the actors of the network. The structure of the distributed ledger and the flow logic of the smart contract are al defined in this document.

## 1.2 Scope

1. Farmers can create an enrollment request to the network
2. Associations approve the request and assign farmers to one among them
3. Farmers can apply for loan
4. Association can approve the farmer’s loan request and upload supporting documents
5. BSI can approve the farmer’s loan request and upload supporting documents
6. Bank ca approve the farmer’s loan request

## 1.3 Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revised by** | **Description of Change** |
| 1.0 | 11-Apr-2022 |  | Initial Draft |
|  |  |  |  |

# 2.0 Environment Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Environment** | **Environment URL** | **Application Installed** | **Owner** |
| 1 |  |  |  |  |

# 3.0 Proposed Design

## 3.1 Assumptions

The following are the assumption of the proposed design document.

1. The blockchain network is designed based on private blockchain frameworks
2. The private blockchain network can define the type and count of consensus participants and approval ratio

## 3.1 Network structure:

The blockchain network for this use-case will be made up of three organizations, listed as follows. Organization in this case denotes a single blockchain node in the blockchain network.

A picture containing diagram

Description automatically generated

Satish Comment : What is the intent of the diagram? Showing the participants? What is does the arrows indicate? It is connecting evert where. Is this intended?

Figure 1- Blockchain Network – participants

**Association**

One or more association can share single organization in the blockchain network, or each of the can have their own organization. The sugarcane farmers will be enrolled and hosted as part of their corresponding association.

**BSI**

BSI is a single organization that can propose the association(s) and bank(s) as part of this solution.

**Bank**

One or more banks can share same organization, or each of them can have their own organization. The bank organization is where the loan application request process flow ends.

**Future expansion**

The network can be expanded to include new association or banks in the future. Any new association or bank that wish to become the part of the blockchain network can submit a proposal request to join. The existing organizations can approve/reject the proposal based on which the new organization will be on-boarded as part of the blockchain network.

The structure of the blockchain network and any proposal to modify it all are openly managed in a distributed manner. The control of the network is distributed equally to all the participants, hence eliminating the central authority.

**Transaction overview**

All the transaction coming into the blockchain network will be processed individually by each organization. The individually process transaction results, from each organization, are then verified by the consensus service for consistency before approving it. Any inconsistency between the transaction results might result in the transaction getting rejected. The result of the transaction is then stored in the immutable ledger. This way all the transactions coming into the blockchain are processed individually by each organization in a true distributed manner. The persistence of the transaction results in the immutable distributed ledger, is handled in the same distributed manner, like transactions.

## 3.2 Smart contracts

Diagram

Description automatically generated

Figure 2- Smart contracts

The smart contract for the loan application request workflow is made up of two different modules.

1. User handling
2. Loan application request

### 3.2.1 User Handling

The user handling module of the smart contract keeps track of all the users in the blockchain network. It is achieved by persisting the public signing key of each user along with the user id in the distributed ledger.

Association organization can use this to enrol different farmers. Each farmer will be provided with a username and RSA signing key pair. The public key will be stored in the ledger. If different banks/ associations share a single organization, then the user handling module can be used to create a username for each bank/association within the organization.

**User Enrolment:**

This part of the smart contract receives the user enrolment request. Each enrolment request contains a unique username to identify the user in the network, type of the user and public signing key from an RSA signing key pair.

The public key along with the user details are persisted in the ledger.

Diagram

Description automatically generated

**User verification as part of transaction:**

This module is called as part of all the transaction request that is coming into loan application request module. Every request by user should be accompanied by an additional field that includes the entire transaction request signed by the user’s private signing key.

Once after receiving the signed transaction request, the module fetches the public signing key of the user from the ledger. The key is then used to verify the signed transaction request, which on successful validation, is passed on the actual transaction module, which is loan application request module in this case.

Diagram

Description automatically generated

### 3.2.2 Loan application request

The loan application request module of the smart contract contains a straightforward approach.

Diagram

Description automatically generated

**Farmer**:

The farmer raises a loan application request. All the details and documents required for the application request is provided by the farmer. Since the blockchain network is distributed. all the organizations can view the loan application request, immediately after it is raised. The documents uploaded can be stored in a normal database or ipfs file system, and the hash of the document is forwarded to the loan application request to the blockchain network.

**Association:**

The association can approve/reject or modify the loan application request, or the information provided by the individual farmer. The association can be restricted to modify the information related to them, in the loan application request. Again, the distributed nature of the blockchain, makes the changes and approval status, available on the network immediately,

**BSI**:

BSI, like association can approve/reject or modify the loan application request, or the information provided by the individual farmer. Restriction can be put in place with the help of the application, to allow BSI to modify the information, only related to them.

**Bank**:

The bank is the destination of the loan application request. The bank can approve/reject a loan application request or send it back to any one of the previous owners for additional clarification.

Due to the distributed nature of the blockchain network, the loan application request can be processed in matter of minutes, rather than the traditional system that takes more time. Blockchain network makes it easier for all the participants, to have a transparent visibility on the application, throughout its lifecycle.

The immutable nature of the blockchain network means, any information that goes into the loan application request, cannot be changed. Any updates to the application request have to come in through transaction, which will be visible for all the organizations.

Satish Comment: If every organization can view the request, then we should recommend a separate organizations for every entity and so not all of them can view all the details (may be breach of privacy), only the organizations that needed to (the association linked to the requester, BSI and the bank(s) who need to see the data for approval) or only part of the transaction can be viewed by everyone (like the name of the requester, loan outstanding and their standing status (delinquent or on track with payments), honestly this is why a credit score is to obfuscate these little details but instead publish only the Credit score without revealing all the underlying details. So, my strong request is to look at this from privacy and security(confidentiality) perspective and fine tune the recommendations. Also, is there separate channels we can create to protect the privacy? Lets think about those aspects of the design as well.