**A close up of a logo

Description automatically generated**

**ASR Belize Project**

Blockchain Design Document

Phase 1

**Table of Contents**

[1.0 Introduction 3](#_Toc101211387)

[1.1 Purpose 3](#_Toc101211388)

[1.2 Scope 3](#_Toc101211389)

[1.3 Version History 3](#_Toc101211390)

[2.0 Environment Details 3](#_Toc101211391)

[3.0 Proposed Design 4](#_Toc101211392)

[3.1 Assumptions 4](#_Toc101211393)

[3.2 Network structure: 5](#_Toc101211394)

[3.2.1 Association 5](#_Toc101211395)

[3.2.2 BSI 5](#_Toc101211396)

[3.2.3 Bank 5](#_Toc101211397)

[3.2.4 Future expansion 6](#_Toc101211398)

[3.2.5 Transactional Channels 6](#_Toc101211399)

[3.2.6 Transaction overview 6](#_Toc101211400)

[3.3 Smart contracts 7](#_Toc101211401)

[3.3.1 User Handling 7](#_Toc101211402)

[3.2.2 Loan application request 9](#_Toc101211403)

# 

# 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. In a blockchain network, an organization is defined as unique single node within the network.
4. For business purpose the Association and Bank are grouped together as one organization each.
5. As a network organization, each association/bank is recommended to host its own organization, for privacy reasons.
6. Organization referred throughout the document is the network organization made up of individual bank/association
7. For convenience purpose, the figures throughout this document is business organization instead on individual network organization
8. Transactional channels, provide a logically separated distributed ledger network, can include one or more network organization
9. A unique transactional channel is created, between different associations and banks on one-to-one basis
10. BSI organization is a default participant of all the transactional channel
11. When unable all the banks/associations can be grouped under a single network organization to save on the deployment cost. Still the transactional channel provides a logically separate network between each organization and banks.

## 3.2 Network structure:

The blockchain network for this use-case will be made up of three organizations, listed as follows. Organization can be defined as follows

1. Business organization – Association, BSI and Bank are the three different business organizations
2. Network organization – Each Association/Bank is made of group of multiple Associations/Banks.

Each association/bank is considered as individual network organization

Diagram

Description automatically generated

Figure - Blockchain Network – participants

### 3.2.1 Association

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

### 3.2.2 BSI

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

### 3.2.3 Bank

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

### 3.2.4 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 network 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.

### 3.2.5 Transactional Channels

Transactional channels provide a logically separated distributed ledger network. Each transactional channel contains one or more network organization. Channels are created between each association and bank in a one-to-one mapping fashion. This way the transaction from one association cannot be accessed by other association, likewise for transaction between banks.

Here is table providing a clear picture of transaction channel combinations, BSI will be part of all the channels listed in the table. Each channel in the table is made up of one network organization from association and one network organization from bank and BSI.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Bank Organizations | | | | | |
| Association Organizations | **Network organizations** | **Bank 1** | **Bank 2** | **Bank 3** | **Bank 4** | **Bank n** |
| **Association 1** | ChannelA1B1 | ChannelA1B2 | ChannelA1B3 | ChannelA1B4 | ChannelA1Bn |
| **Association 2** | ChannelA2B1 | ChannelA2B2 | ChannelA2B3 | ChannelA2B4 | ChannelA2Bn |
| **Association 3** | ChannelA3B1 | ChannelA3B2 | ChannelA3B3 | ChannelA3B4 | ChannelA3Bn |
| **Association n** | ChannelAnB1 | ChannelAnB2 | ChannelAnB3 | ChannelAnB4 | ChannelAnBn |

### 3.2.6 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.

## 3.3 Smart contracts

Diagram

Description automatically generated

Figure - 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

### 3.3.1 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. Based on the association the farmer belongs to, the bank to which the loan application request is made, the transaction channel will be selected, and the transaction is forwarded. This makes the loan application request visible to only the following network organizations, the association the farmer belongs to and the bank to which the application is addressed.

**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. The BSI being eligible to view all the transactions, can provide a financial score for the farmer, based on their previous loan application. This is determined by the on-time payment of interest and proper closure of the loan application by the farmers.

**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.

Once the application request is approved, the banks can keep updating the status of the loan application. This is achieved with a help of additional field in the loan application request managed by the bank, based on the action of farmers such as,

* On time payment of interest
* Late payment of interest
* Default of loan application

This field provides additional insights to BSI, on farmer’s credit performance for the current loan. This can also be used on decision making by BSI for the farmer’s future loan application request.

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 must come in through transaction, which will be visible for all the organizations.