NKDA Birth/Death Registration on Blockchain

Securing Birth/Death Records Immutably

.

Table of Contents

[Executive Summary 2](#_Toc534293452)

[1.1 Background 2](#_Toc534293453)

[1.2 What is blockchain? 2](#_Toc534293454)

[1.3 Blockchain solution for birth/death records: 3](#_Toc534293455)

[1.4 Advantages: 4](#_Toc534293456)

[1.5 Integration Architecture: 4](#_Toc534293457)

[Service Integration Details:- 6](#_Toc534293458)

[2.1 Other Service Integration Details 6](#_Toc534293459)

[2.1.1 Birth/Death Registration Service 6](#_Toc534293460)

[Hardware Requirements 9](#_Toc534293461)

[Conclusion 10](#_Toc534293462)

# Executive Summary

## Background

Webel is keen to explore the strengths of blockchain to inculcate trust and transparency for residents and businesses housed within New Town area of Kolkata under New Town Kolkata Development Authority (NKDA). One of the key objectives was bringing transparency in every stage of the citizen lifecycle, and creating an immutable, tamper proof, robust system of birth/death records was identified as the first endeavor to leverage the power of blockchain.

The creation of an immutable archive or records, with complete traceability of information was facilitated by the use of blockchain.

## What is blockchain?

Blockchain is a digital, decentralized (distributed) ledger (database) that keeps a record of all transactions that take place across a peer-to-peer network. It is an interlinked and continuously expanding list of records stored securely across a number of interconnected systems. This makes blockchain technology resilient since the network has no single point of vulnerability. Additionally, each ‘block’ is uniquely connected to the previous blocks via a digital signature which means that making a change to a record without disturbing the previous records in the chain is not possible, thus rendering the information tamper-proof. The key innovation in blockchain technology is that it allows its participant to transfer assets using internet protocol and without any centralized third party (intermediary).

A node is simply a computer server that is connected to a network. When a node connects to a network for the first time, it downloads the copy of the ledger.

Node 1

Node 2

Node 6

Node 4

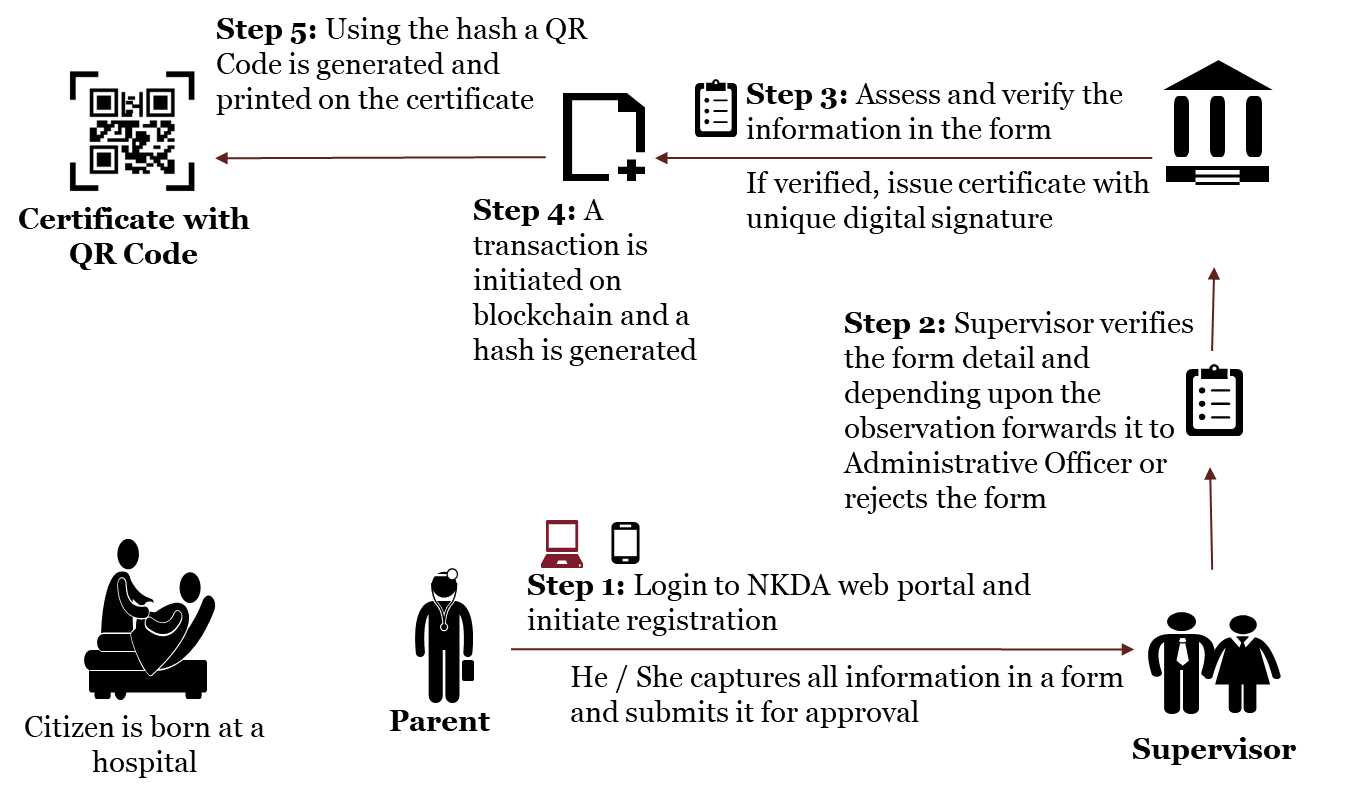
Node 5

Node 3

Ledger is basically a chain of blocks where each block points to it previous block with a hash pointer, thus blockchain. Each block contains valid transaction data.

## 1.3 Blockchain solution for birth/death records:

Blockchain technology can help store birth/death registration data in an immutable fashion with a time stamp at which it was created. Once the data has been recorded in the blockchain it cannot be altered/deleted. The birth/death data can be verified by querying the blockchain.



All relevant data of the child will be captured from the form submitted by the parent and if Administrative Officer approves the request will be stored as transaction metadata in the blockchain.

Similarly, for death registration once the records are verified by the authorities a transaction is initiated on the blockchain network. The record is sent back and printed on the death certificate in for of QR code.

Any person/organization with the birth certificate can check the authenticity of the document by scanning the QR Code printed on the certificate using NKDA mobile application. When the QR code is scanned the mobile application will search the encrypted block data and transaction hash and will print the data related to the certificate. If the certificate has been tampered in any manner application will notify the user about the same. There will be a time stamp attached to each record which can help trace the certificate and know if it existed in past.

## 1.4 Advantages:

Blockchain streamlines the entire birth/death registration process, makes the system transparent, establishes trust and prevents forging of certificates.

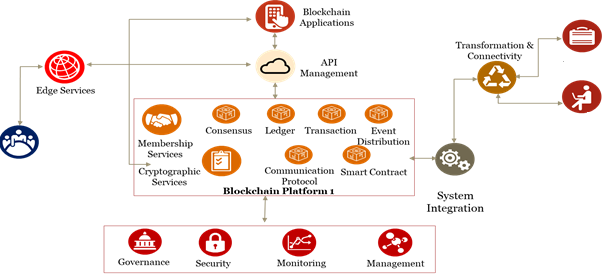
Verification

Trust

Immutability

* Quick and easy verification of certificates using application
* Once data has been stored in blockchain it cannot be altered or modified thus creating an air tight birth registration system.
* System will be fraud free as the data can be hacked/modified thus creating a sense of trust in the system.
* Duplicate certificates will be eliminated altogether

## Integration Architecture:



* Connectors
* Customized APIs
* Micro-services

Developers

Administrator

Operators

Auditors

Govt. Officials

Blockchain Id

3

2

Birth/Death Data

Blockchain Platform

Data and Token for authentication

1

E-District

JWT  
(Authenticate using token)

***Data flows across the Solution Implemented for Birth/Death Records***

Service Integration Details: -

This is a blockchain based record for birth/death registrations under West Bengal e-District. In existing e-District system, the birth/death registration service has a number of functionalities (Save Birth/Death Record, Check Birth/Death Record and Print Birth/Death Certificate).

**Save Birth/Death Record**: - All the input details for the birth registration are entered from e-District system, then supervisor captures all the information for the verification and forwards it to administrative officer. After verification, the administrative officer’s data is consequently saved on the blockchain system which triggers the generation of a blockchain id.

**Check Birth/Death Record**: - To retrieve a birth/death record from the system user needs to provide the blockchain id as the input which would generate details of the birth/death registration

Following are the key architecture decisions taken for Birth/Death Registration service integration:

* Blockchain API Integration
* JWT Authentication

## Other Service Integration Details

### Birth/Death Registration Service

Citizen can perform following operations:

* Save Birth/Death Record
* Check Birth/Death Record
* **Integration Type** – API based (REST Service)
* **Technology used**- Blockchain (Multichain Blockchain which has four nodes), Node JS, Sql Server 2017, JWT.
* **Service Details**- In this service Blockchain API have JWT authentication for accessing API only for a single user account with single role. First e-District system should get JWT token from developed solution using user details input which is mentioned below. After getting JWT token e-District system passes the token when accessing the Blockchain API for saving birth/death record into the Blockchain system. Then JWT server verifies the token which is passed from e-District system. If the verification is successful, then data is pushed into blockchain. After that as a response e-District system gets a transaction hash. The e-District system will get a birth/death record from the Blockchain system using that hash only. This hash is also used to create the QR Code which is printed on the certificate (This part of printing the QR code using the hash has been developed in e-District system).

#### **API for Get JWT Token**

|  |  |
| --- | --- |
| **Service Description** | ***Get JWT Token for API Authentication*** |
| **REST API Details** | [Birth registration: http://202.61.117.207:8545/getToken](file:///C:\Users\nsarkar007\Downloads\Birth%20registration:%20http:\202.61.117.207:8545\getToken)  Death registration: http://202.61.117.207:8443/getToken |
| **Method** | POST |
| **Input** | **Content-Type**:- application/x-www-form-urlencoded  **Body**: - email:aofficer@webel.com  password:Zzwisfbuzh4tQ@25  phone:9804567248  rolename:aofficer |
| **Input Parameter Description** | Email: - Registered user’s email id.  Password: - Registered user’s password.  Phone: Registered user’s mobile number.  Role name:- Registered user’s role name. |
| **Output** | Ex:- {  "token": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxLCJpYXQiOjE1NTM2Nzc0NzYsImV4cCI6MTU1MzY3ODA3Nn0.13QDJ1sPhDO6uTP8lg-hCFhCJKZV\_Roqk23LaBCliIQ",  "success": true  } |
| **Output Parameter Description** | token:- JWT token |

#### **API for Save Birth/Death Record**

|  |  |
| --- | --- |
| **Service Description** | ***Save Birth/Death Record*** |
| **REST API Details** | [Birth Registration: **http://202.61.117.207:8545/saveBirthDetail**](file:///C:\Users\nsarkar007\Downloads\Birth%20Registration:%20http:\202.61.117.207:8545\saveBirthDetail)  Death Registration: **http://202.61.117.207:8443/saveDeathDetail** |
| **Method** | POST |
| Input | **Content-Type**:- application/xml  Example for Birth regisrtration:  var settings = {  "async": true,  "crossDomain": true,  "url": "http://202.61.117.207:8545/saveBirthDetail",  "method": "POST",  "headers": {  "Content-Type": "application/xml",  "Authorization": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxLCJpYXQiOjE1NTM2Nzc0NzYsImV4cCI6MTU1MzY3ODA3Nn0.13QDJ1sPhDO6uTP8lg-hCFhCJKZV\_Roqk23LaBCliIQ",  "Cache-Control": "no-cache"  },  "data": "<Appl\_Data>  <Meta>  <Appl\_Nm>Akshita Singh</Appl\_Nm>  <Appl\_Dt>1995-11-23 20:45:40.187</Appl\_Dt>  </Meta>  </Appl\_Data>"  }  $.ajax(settings).done(function (response) {  console.log(response);  }); |
| **Input Parameter Description** | Input body as XML format of Birth/Death Data |
| **Output** | Transaction Hash (eg-43ec0d525fded38669208fd5db59279bee97e4888ca6e35b82315dffa00a57cd) |
| **Output Parameter Description** | Blockchain Id |

#### **API for Get Birth Record**

|  |  |
| --- | --- |
| **Service Description** | ***Get Birth Record*** |
| **REST API Details** | Birth Registration: [**http://202.61.117.207:8545/**getBirthData](http://13.127.236.20:8545/getBirthData)  Death Registration: **http://202.61.117.207:8443/getDeathData** |
| **Method** | GET |
| **Input** | Content-Type:- application/xml  **Parameter:-** 43ec0d525fded38669208fd5db59279bee97e4888ca6e35b82315dffa00a57cd |
| **Input Parameter Description** | **Parameter:-** Blockchain Id |
| **Output** | <Appl\_Data><Meta><Serv\_Id>102</Serv\_Id><Appl\_Nm>Mr. Sahajan Jawed</Appl\_Nm><Appl\_Dt>2018-10-30 22:46:40.187</Appl\_Dt></Meta></Appl\_Data> |
| **Output Parameter Description** | Birth/Death data |

# Hardware Requirements

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Component | Unit | Core (Per Unit | Core (Total) | RAM (GB)(Per Unit) | Hard Disk (GB) (Per Unit) | Total Disk (GB) | OS/Software Required |
| App Server | 2 | 4 | 8 | 16 | 250 | 500 | (Ubuntu 16.04 LTS) & node.js (v8.11.2) |
| Blockchain Node | 4 | 4 | 16 | 32 | 300 | 1200 | Ubuntu 16.04 LTS |
| SQL | 1 | 8 | 8 | 16 | 250 | 250 | SQL Server 2014 express edition (OS - MS Windows 2016 Std) |
| Total | |  |  |  |  | 1950 |  |

|  |  |  |
| --- | --- | --- |
| Blockchain Framework | Version | No of Ubuntu Node to be installed in |
| Multichain | v1.0.6 | 4 |

|  |  |  |
| --- | --- | --- |
| Sl No | Software/Service Requirement | Qty |
| **1** | **License: Ubuntu 16.04 LTS** | **As Required** |
| **2** | **Load Balancer** | **1) One for App Servers 2) One for Blockchain Nodes** |
| **3** | **SSL** |  |

# Conclusion

The Blockchain solution provides value by improving processes associated with birth/death registration and real transactions. The following is a brief list of some of these improvements:

* Eliminating the need for physical archives of birth/death registration.
* Increased resilience and redundancy of the transactional data in the birth/death registry.
* Greater security for users of the system, in part because cryptographically secure system.
* Faster and more transparent transactions.
* Making it possible to verify authenticity on blockchain.
* Fraud free system. Making it more difficult to forge certificates.

Blockchain technology can play a key role in embracing trust and transparency in the birth/death registration process in addition to increasing the security of the system. It eliminates counterfeiting and attacks through transparency and use of cryptographic primitives for authentication.