REQUEST FOR EXPRESSIONS OF INTEREST
CONSULTING SERVICES

Selection #: RG-T3321-P002
Selection Method: Full Competitive Selection
Country: Regional - Caribbean
Sector: Social Sector
Funding – TC #: ATN/OC-16942-RG
Project #: RG-T3321
TC name: Blockchain-based Academic Passport for the Caribbean
Description of Services: design and implementation a regional blockchain-based solution to issue and manage CXC's credentials

Link to TC document: http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=EZSHARE-232292182-6

The Inter-American Development Bank (IDB) is executing the above-mentioned operation. For this operation, the IDB intends to contract consulting services described in this Request for Expressions of Interest.
Expressions of interest must be delivered using the IDB Portal for Bank Executed Operations (http://beo-procurement.iadb.org/home) by: **February 11th 2020, 5:00 P.M.** (Washington D.C. Time).

The consulting services ("the Services") include building a standardized but customizable digital solution that leverages blockchain technology for the issuance and verification of certificates and data associated with the CXC's students, as well as develop the capabilities needed to add new countries into the Regional Blockchain Educational Credentialing solution and to enhance the implementation of CARICOM's free movement of skills.
The estimated timeframe for the performance of such services is estimated to be completed by the end of fourth quarter of 2020.

Eligible consulting firms will be selected in accordance with the procedures set out in the Inter-American Development Bank: *Policy for the Selection and Contracting of Consulting firms for Bank-executed Operational Work* - GN-2765-1. All eligible consulting firms, as defined in the Policy may express an interest. If the Consulting Firm is presented in a Consortium, it will designate one of them as a representative, and the latter will be responsible for the communications, the registration in the portal and for submitting the corresponding documents.

The IDB now invites eligible consulting firms to indicate their interest in providing the services described below in the draft summary of the intended Terms of Reference for the assignment. Interested consulting firms must provide information establishing that they are qualified to perform the Services (brochures, description of similar assignments, experience in similar conditions, availability of appropriate skills among staff, etc.). Eligible consulting firms may associate in a form of a Joint Venture or a sub-consultancy agreement to enhance their qualifications. Such association or Joint Venture shall appoint one of the firms as the representative.

Interested eligible consulting firms may obtain further information during office hours, 09:00 AM to 05:00 PM, (Washington D.C. Time) by sending an email to: Fernando Yitzack Pavon – *fernandop@iadb.org*

Inter-American Development Bank
Division: Labor Markets & Social Security
Attn: Fernando Yitzack Pavon, Program Team Leader

1300 New York Ave, NW, Washington DC 20577, USA
Tel: + 202 312-4273
E-mail: *fernandop@iadb.org* / *taniag@IADB.ORG*
Web site: www.iadb.org

Draft Summary of Terms of Reference on next page.

TERMS OF REFERENCE - STATEMENT OF WORK FOR BLOCKCHAIN STRUCTURE FOR CREDENTIALS AT CXC

Blockchain-based Academic Passport for the Caribbean (RG-T3321)

January 2020

TABLE OF CONTENTS

Abbreviations

IDB	Inter-American Development Bank
IDB Lab	Innovation Lab of the IDB
SCL	Social Sector at IDB
LMK	Labor Markets Division at IDB
CARICOM	Caribbean Community
CSME	Caribbean Single Market Economy
CXC	Caribbean Examinations Council
CSEC	Caribbean Secondary Education Certificate
CAPE	Caribbean Advanced Proficiency Examination
CPEA	Caribbean Primary Exit Assessment
CCSLC	Caribbean Certificate of Secondary Level Competence
CVQ	Caribbean Vocational Qualification
CXC-AD	CXC Associate Degree
EPS	CXC's Examination Processing System
ORS	CXC's Online Registration System
MOE	Ministry of Education
UWI	University of the West Indies
ACTT	Accreditation Council of Trinidad y Tobago
GDPR	General Data Protection Regulation
LMT	Learning Machine Technologies
EY	Ernest and Young
TOR	Terms of Reference

1. Introduction

The purpose of this document is to provide prospective providers with the information needed to present an implementation and support proposal for “Regional Educational Credentialing for the Caribbean Advanced Proficiency Examination (CAPE) at the Caribbean Examinations Council (CXC)” using blockchain technology.

Traditionally, CXC has relied on a paper-based system for the issuance of certificates and provision of results. However, the organization has recognized the global shift to utilize digital tools, such as blockchain-enabled solutions, in the delivery of credentialing and related services. As such, in CXC decided to carry out a blockchain-based initiative with the support of the IDB to digitalize the issuance and management of academic credentials under the purpose of improving efficiency, traceability, interoperability and scalability. This initiative is widely known and will be referred to in this document as “the Blockcerts initiative for the Caribbean”.

During August 2018, CXC hired a vendor, Learning Machine Technologies (LMT), to deliver an initial pre-pilot in Barbados to test and validate the fit of blockchain technology for the goals described, and identify the challenges to be overcome for a full productive and scalable solution. It aimed to allow students to create a digital wallet containing their provable academic achievements. It also aimed to allow these institutions to leapfrog the digitization process, and to address many of the interoperability issues associated with legacy digital formats such as PDF. The contract with LMT expired on August 2019. At present, CXC intends to develop and expand their own solution, leveraging the lessons learned from the pre-pilot. A detailed description of the pre-pilot and its evaluation is presented in Annex A.

Following this first phase, CXC hired a vendor, Ernest and Young (EY), to deliver an assessment on the pre-pilot and a roadmap to implement a scalable and productive blockchain-based solution to issue and manage CXC’s academic credentials over the Caribbean. This second phase was concluded in November 2019.

At present, CXC is in seeking a vendor to execute the third phase of the initiative, consisting of the design and implementation a regional blockchain-based solution to issue and manage CXC’s credentials leveraging all the lessons learned from the first and second phases.

This document includes the highlights of the pre-pilot, background, objectives and challenges of the project. It also states the technological requirements, expected outputs and specify the functionalities that should be accomplished.

2. Background and Justification

2.1. Caribbean Examinations Council

The Caribbean Examinations Council (CXC) is a regional examining body that provides examinations for secondary and post-secondary candidates in Caribbean countries and award certificates and diplomas on the results of any such examinations so conducted.

The CXC’s mission is to provide the region with:

Syllabuses of the highest quality; valid and reliable examinations and certificates of international repute for students of all ages, abilities and interests;
Services to educational institutions in the development of syllabuses, examinations and examinations administration in the most cost-effective way.

CXC comprises 16 English-speaking participating countries: Anguilla, Antigua and Barbuda, Barbados, Belize, British Virgin Islands, Cayman Islands, Dominica, Grenada, Guyana, Jamaica, Montserrat, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Trinidad and Tobago and Turks and Caicos Islands.

CXC offers a suite of qualifications examinations to meet the needs of the region:

Caribbean Secondary Education Certificate® (CSEC®),
Caribbean Primary Exit Assessment™ (CPEA™),
Caribbean Certificate of Secondary Level Competence® (CCSLC®),
Caribbean Vocational Qualification (CVQ),
Caribbean Advanced Proficiency Examination® (CAPE®)
CXC® Associate Degree (CXC®-AD).

CXC has, over more than 40 years of service to the region, contributed significantly to ensuring high standards of examination preparation, administration and certification for students transitioning from secondary to tertiary levels and accessing the labor market. CXC ultimate objective is to produce a larger, certified, globally competitive workforce across the Caribbean.

2.2. CARICOM and CSME Agenda

The Caribbean Community (CARICOM) is an organization of fifteen Caribbean nations and dependencies having primary objectives to promote economic integration and cooperation among its members, to ensure that the benefits of integration are equitably shared, and to coordinate foreign policy. The table below gives a list of countries, associated countries, organizations, and bodies that make up the CARICOM.

CARICOM aims to facilitate the free movement of goods, services, capital and technology of the Caribbean Single Market Economy (CSME).

The CSME as a concept, originated in 1963 with the Caribbean Free Trade Agreement which allowed the removal of tariffs. This arrangement then progressed to the Treaty of Chaguaramas which enabled and supported a single common market, the free movement of goods and capital, and the right to establish a business (CARICOM Secretariat, 2019). One of the important aspects of CSME is the movement of persons and the Certificate of Recognition is the mechanism used to facilitate this.

Currently, persons who apply to the CSME for the Certificate of Recognition include university graduates, artists, musicians, media workers and sports persons. To obtain this Certificate of Recognition, persons must apply in their home country and once approval is received from that country, their qualifications must then be verified again by the member state in which the applicant wishes to reside. Therefore, the CXC' blockchain solution can be designed to support this strategic evolution by using the individual's lifelong record of credentials.

Countries	Associated Countries	Organizations	Bodies
Antigua and Barbuda	Anguilla	The Conference of Heads of Government	Legal Affairs
Bahamas	Bermuda	The Community Council of ministers	Budget Committee
Barbados	British Virgin	The Council of Trade and Economic Development	Committee of Central Bank Governors
Belize	Islands	Council of Foreign and Community Relations	
Dominica	Cayman Islands	Council of Human and Social Development	
Grenada	Turks and Caicos Island	Council for Finance and Planning	
Guyana		Council for Nation Security and law enforcement	
Haiti			
Jamaica			
Montserrat			
St Kitts and Nevis			
St Lucia			
St Vincent and the Grenadines			
Suriname			
Trinidad y Tobago			

Table 1. CARICOM composition.
Source: CARICOM Secretariat 2014

CARICOM's Strategic Plan for 2015 to 2019 identified eight integrative priorities, namely:

Building social resilience
Building economic resilience
Building environmental resilience

Building technological resilience
Strengthening the CARICOM identity and spirit of community
Strengthened community governance
Coordinated Foreign Policy
Research and Development and Innovation

2.3. Blockchain-based solution for credentialing

The biggest challenge with the process to obtain the Certificate of Recognition is the duration taken. Countries across the Caribbean have expressed concerns with the implementation of the CSME with regards to the “free movement of people”.

According to an article in the Jamaican Observer, Caribbean countries are facing problems with the process of acquiring the Certificate of Recognition as it is not optimized. To obtain the Certificate of Recognition, persons must apply in their home country. Once approval is received from that country, their qualifications must then be verified again by the member state in which the applicant wishes to reside. Therefore, every candidate’s credentials are verified twice, once by their home country and a second time by the member state in which they wish to reside. This process does not support the CARICOM’s strategic priority described previously.

Blockchain technology allows to create decentralized an immutable register of information where information can be trusted and validated. Blockchain networks can be used to record the cryptographic proofs of the digital identity of entities and persons and the validity of digital credentials that are issued to them.

Completing the CARICOM “Application for Certificate of Recognition of Caribbean Community Skills Qualification” (Certificate of Recognition) process is long. Although not CXC’s core business, there are significant opportunities to use a blockchain technology to improve the process of obtaining the Certificate of Recognition.

If the regional blockchain credentialing is implemented properly, it can eliminate some of the current challenges faced by citizens of the region. Blockchain credentialing can be used to support a regional digital identity of Caribbean citizens, which can enable the CSME certification of recognition process. As an example, this can be done by the introduction of a self-sovereign identification system through which each applicant is given a decentralized identifier (DID). The issuing bodies in home country of the applicant would be the issuer of verifiable certificates (VC), the issuer would use the credential definitions and schemas on the ledger to construct the VC. This issuer would sign this VC and send to the identity owner. The relevant bodies in the member state countries can verify the authenticity of these certificates by validating cryptographic proofs on the ledger against the certificate.

Blockchain technology can play an important role in the validation of the certificate, helping prove that the certificate is genuine and issued to the correct individual. There are multiple ways in which blockchain technology can provide this. The simplest method to implement would be to use a blockchain to record a cryptographic proof of a record. In this approach, a student would be issued with a digital certificate by the governing body, and this certificate would be stored in an off-chain system (not on a blockchain). At the time of issuance to the student, the governing body would also make a cryptographic proof of this certificate and store this on a blockchain, creating an immutable proof of what has been issued and to whom. Thus, when presented with the off-chain certificate, an interested party can

immediately validate the provenance and authenticity of the off-chain certificate by simply interrogating the cryptographic proof on the blockchain. This process should be able to be done by the interested party, without any reliance on third party software or systems that allow them to independently perform the validation. A way of implementing this is presented in Section 5.

If an appropriate process is implemented, it has the potential to improve the CSME Certificate of Recognition application experience while reducing processing time. The member state in which the candidate wishes to reside can more easily process their application if their credentials are already verified and accessible on a secure blockchain. Validation of the Certificate of Recognition and underlying academic or vocational credentials by potential employers, immigration departments, etc. can then be performed securely and electronically. This would then reduce the time spent on authenticating certificates, which have already been validated at the point of original application. If the platform is deployed openly using a public blockchain, then institutions outside the region can also use this same platform to add certificates for those students studying abroad.

Regardless of the exact approach taken, the guiding principles behind the deployment should be distribution and decentralized. No one party or organization should be the only way to either validate or store credentials. Likewise, the blockchain itself will also need to be chosen such that no one party controls the network and it is deployed at sufficient scale to be a distributed platform.

It is noted that the Prime Minister of Barbados supported the use of blockchain technology to improve the CSME process in her address to CARICOM in 2018. She described the CSME applicants as being victims of long processing timelines and declared that this problem can be solved by the using blockchain technology. The implementation of blockchain technology would therefore assist CARICOM in building a society that uses technology to create a digital economy, consistent with its goals.

2.4. The Inter-American Development Bank and the strengthening of employment and training services

The Labor Market Division of the Social Sector (SCL/LMK) of the Inter-American Development Bank (IDB) promotes more and better jobs in Latin America and the Caribbean. The IDB aims to achieve regional goals in poverty reduction, equity of opportunities, and improvement of labor productivity, through the strengthening of employment and training services, improvement in the design and scope of social security, and analysis of labor markets and labor information. To achieve these goals, the IDB is currently focusing on analytical work and projects in the following four main areas: Intermediation, Labor Training, Labor Force Migration and Social Security.

2.5. LACChain

The Innovation Lab of the Inter-American Development Bank (IDB Lab) is leading a global Alliance to develop the blockchain ecosystem in Latin America and the Caribbean named LACChain. The purpose of this project is to foster integration and development and achieve social impact within the Caribbean and Latin American Community through the use of blockchain technology.

LACChain has developed and is maintaining and offering to test blockchain networks that several entities and blockchain-initiatives in the Region are using. Additionally, LACChain is addressing several issues related to the use of blockchain technology as the absence of standards and regulations, limited

collaboration between actors in the systems, inexistent or unclear regulatory policies, data privacy, identification and authentication of users, governance or transactional fees.

EY advised that "*by using technologies like LACChain, the region may be able to enhance its competitiveness and move towards smart digital communities where Caribbean citizens have access to technology building blocks which will allow them to create their own digital identity. In addition to building smart societies, this technology has the potential to facilitate greater integration of services that individual Caribbean governments provide, for example the CSME Caribbean Single Market "Certificate of Recognition*".

3. CXC's credentialing processes

CXC's credentialing processes can be divided into four stages in the context of its possible evolutionary path to support the CSME, as illustrated in Figure 1.

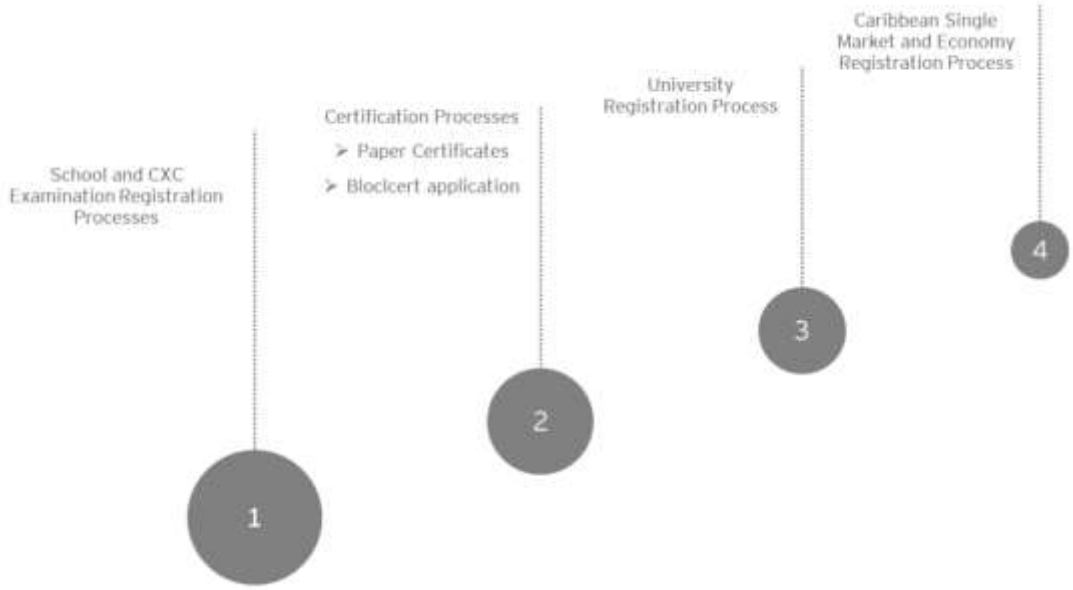

Figure 1. Evolution of CXC Credentialing Processes

3.1. Secondary schools and CXC Examination Registration Processes

The typical process for registering students for CXC examinations across the Caribbean entails the schools' administrators manually collecting student data and entering it into CXC's Online Registration System (ORS). The related process flow for all countries is shown in Figure 2.

Some of the information collected during this process is required for the credentialing blockchain solution, including the unique identifier for the student, which can vary by country. The design of the blockchain platform would therefore include an appropriate interface with the ORS. The information entered on the ORS is then available for the Ministry of Education in the relevant country.

The main pain point with the internal registration process lies with the issuing of internal registration forms to students. This process takes the longest because it is usually done manually. The average time taken to issue and complete this process is three weeks. This delay often occurs due to poor penmanship, incomplete forms, or the long time that administrators take to ensure that the information entered is accurate.

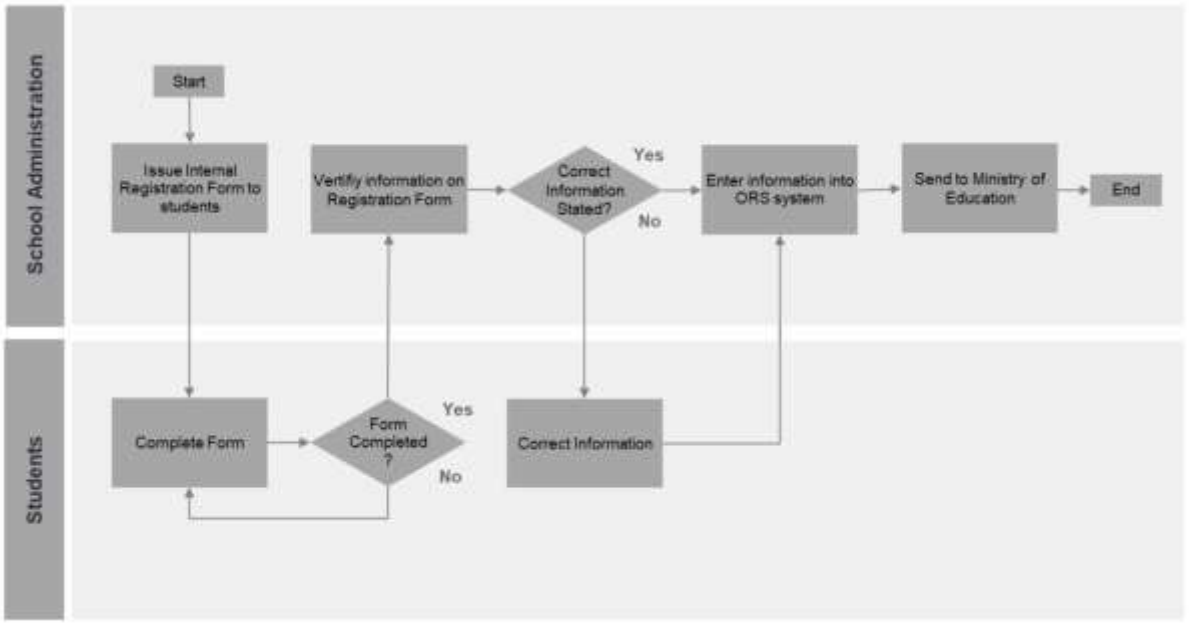

Figure 2. Typical examination registration process at secondary schools

In addition, some schools do not enforce the use of Government-issued identification in the registration process. This can result in candidates using alternative names during registration which then creates problems with the issuance of examination timetables.

3.2. CXC Examination registration process

The Ministry of Education reviews this information and once satisfied, forwards it to the CXC's Registration Unit. This Unit enters the information into their Examination Processing System (EPS) as shown in Figure 3 below.

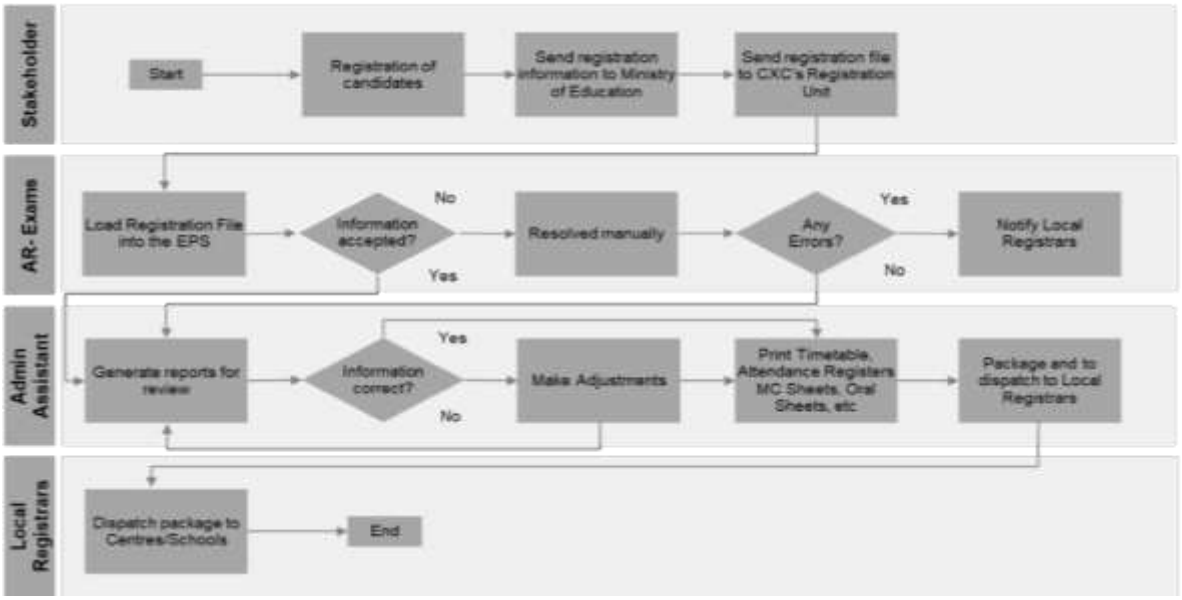

Figure 3: Typical CXC registration of examination candidates

In addition to the registration of candidates, it is necessary to produce a series of printed documents for delivery to the candidates, which includes timetables, attendance registers and oral sheets.

There are several pain points with this process. For example, because of the manual registration process that occurs in schools, this results in multiple unforeseen human inputs, leading to incorrect demographic information being entered in the EPS i.e. spelling errors or incorrect candidate names, addresses etc. AR- Exams personnel must then manually resolve these issues by either contacting the local registrar[1] or sorting through the given information. The timeline for resolution of this pain point varies but causes severe bottlenecks in process.

And finally, candidates are given a new candidate number for every sitting of exams; therefore, on the EPS system, one person can have several candidate profiles which can introduce significant bottlenecks in the system.

3.3. CXC certification process

Currently, CXC provides paper-based certificates to all students with the option to obtain an additional e-certificate using the LMT pre-pilot solution. The current paper- based certification process involves the printing and distribution of certificates as illustrated in Figure 4. In this process, CXC issues preliminary examination results by mail to students giving them the option, following an approved process, to make corrections such as spelling errors in names. Finally, after proper checks are made and queries resolved, paper certificates are printed and distributed to students in each member country.

[1] Local registrars are employees that work at the Ministry of Education.

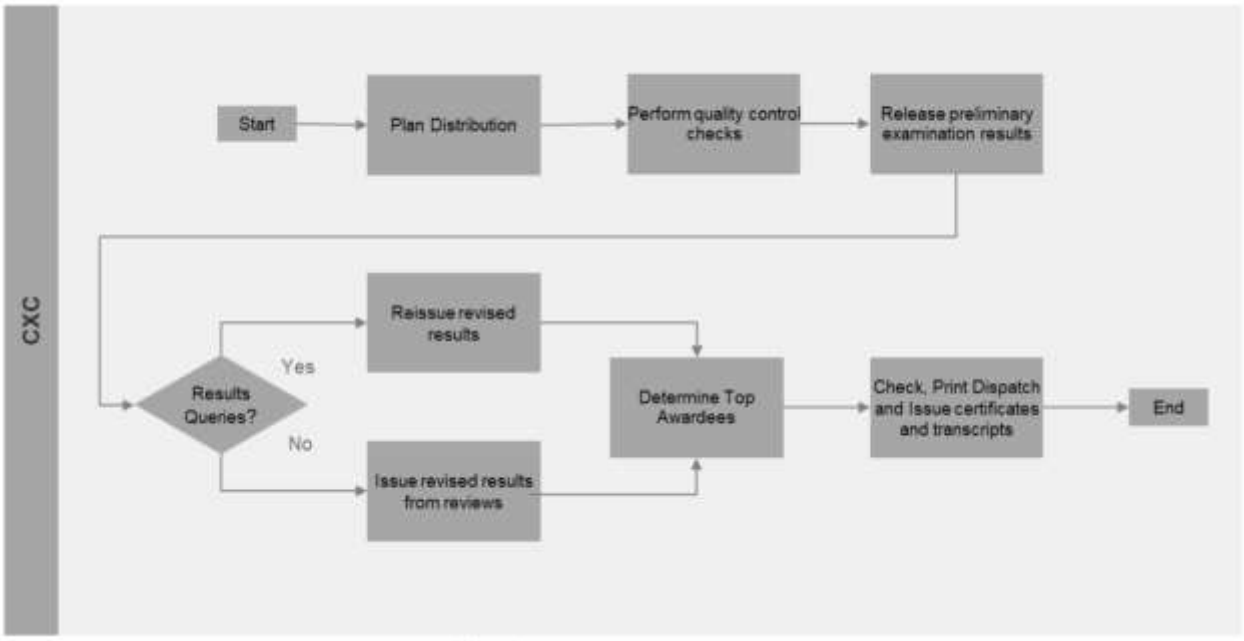

Figure 4. CXC's current paper-based certification process

We have also documented CXC's current process for the issuance of e-certificates via the LMT pre-pilot solution as shown in Figure 5.

The verifier in the pre-pilot would be the universities and employers. The key pain point in this process arises from the fact that currently the issuer sends the blockchain credentials via a URL. This can be easily imitated and therefore can cause fraud and decrease the reputability of CXC e-certificates.

The average age of a CXC CSEC candidate, holder of certificates, is about 15 or 16 years which is under the legal age of consent. Therefore, a parent or guardian must be responsible for candidates' data until they are of legal age. The current Learning Machine solution does not address the issue of transferring of ownership of the e- certificate.

The handing of this Self-Sovereign Identity (SSI) is very important because it is a lifelong identity and ensuring proper management is important. Hence it would be very plausible that parent and guardians have control over this. In this case the parent or guardian would be considered as a third-party holder of their child's Verifiable Credential. The verifier of the credentials must be aware of who is presenting the VC because this can cause fraud and false claims. Therefore, the verifier must validate the holder of the VC and verify their right to present the credentials. In conclusion, the parents may need to have a decentralized identifier themselves to be legally responsible for their child's data.

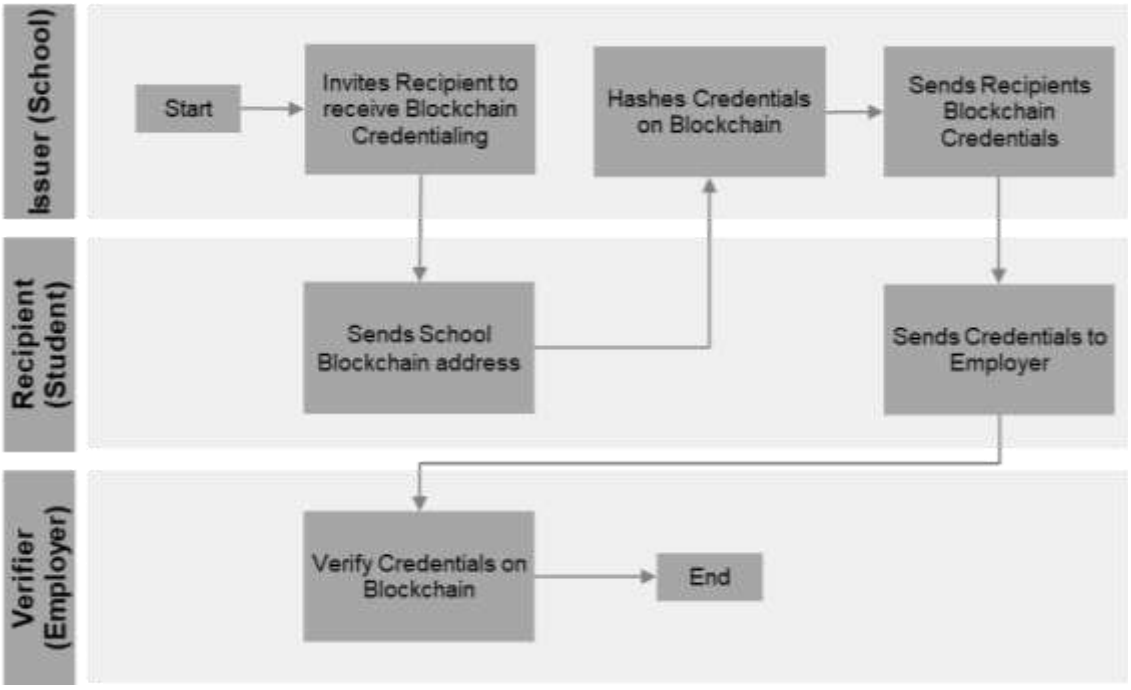

Figure 5: CXC's current blockchain-based credentialing process

3.4. University registration process

The University of the West Indies (UWI) is integrated into the operations of CXC as it relates to students' results and transcripts to allow it to make its admission decisions. UWI receives applicant's examination results from CXC via a text file as illustrated in Figure 6. This file is then uploaded as necessary into the UWI's IT systems. If the student is applying outside of the current CAPE results period, the UWI manually enters that student's results, as it will not be available from the current data in ORS/EPS. There are pain points associated with the current UWI process. For example, in some cases, UWI must manually locate candidates results. The timespan for getting results and issuing acceptance letters is short (approximately 2 weeks), therefore time spent on manually locating students' records negatively impacts the process.

It is noted that CXC offers the provision of this text file service to UWI only. However, with improved technology, this service can be an additional business opportunity for CXC which they can offer the other universities and institutions in the Caribbean. Students can be asked to indicate which university or institution they would like to receive their verified credentials, and with the appropriate technology, this request can be serviced electronically. There is the potential for this capability to become a fee-based service for universities or colleges wanting early access to results data. This could also be further extended to permissioned marketing opportunities and analytics, again for a fee. It should also be possible to allow universities to publish certificates using their own platforms. In the long term, CXC can look at extending their platform to allow universities to be issued their own decentralized identifiers (DID). With this arrangement, universities would be able to issue verifiable credentials VC to students. CXC can build the infrastructure and allow other third parties on the platform for a fee.

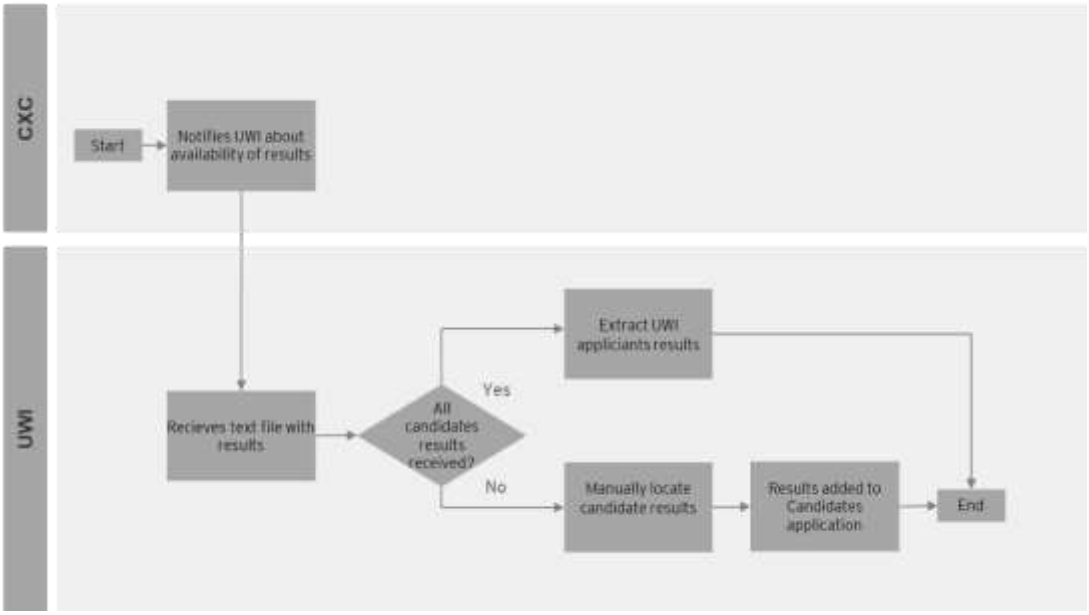

Figure 6. UWI registration process relative to CXC results

3.5. CSME application process

The current CMSE process includes the verification of qualifications by the relevant accreditation body in each country. This information in then used as an input into the CSME application process as shown in the Figure 7. Once the CMSE application is approved in the home country, this process is repeated for the member state in which the candidate wishes to reside.

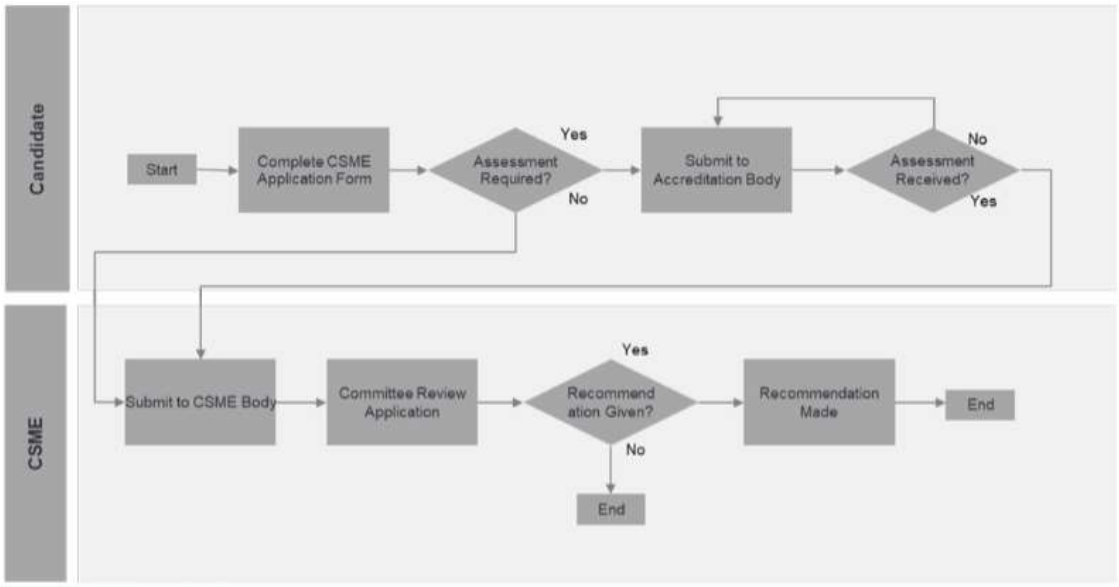

Figure 7. CSME Application process

The main challenge is that there is no integral mechanism or tool for the issuance nor for the validation of certificates by different users in an automated, secure, real-time manner in the Caribbean region. The problems that arise from this challenge are:

- There is no alignment to CARICOM's strategy priority related to improving competitiveness and innovation by Building Technological Resilience and creating Digital Citizens.
- There is no optimized process; they have tedious and long processing timelines.
- There is no efficient process because one person can have several candidate profiles when they have more than one exam.
- There is no transparent accessibility either traceability of the data.
- Because of the manual process in some process phases, many errors result, i.e. spelling errors, incorrect names, addresses, etc.

Other challenges that arise from the pre-pilot:

- Potential security risks associated with unauthentic records, from the fact that currently the issuer sends the blockchain credentials via a URL. This can be easily imitated and therefore can cause fraud and decrease the reputability of CXC e-certificates.
- There is no capacity to ensure relevant data protection, confidentiality and privacy regulations or laws adhered to.
- There is no ledger distribution due to the limited number of nodes in the initial implementation.
- Identity and access management, and the issues around changing wallet ownership, sharing wallets etc. There is no transferring of ownership of the e- certificate. The average age of a CXC CSEC candidate, holder of certificates, is about 15 or 16 years, which is under the legal age of consent. Therefore, a parent or guardian must be responsible for candidates' data until they are of legal age.
- Lack of interoperability with other systems or platforms within CXC and its external stakeholders.
- Engagement with citizens.

4. Objective

The objective of this consultancy is to build a standardized but customizable digital solution that leverages blockchain technology for the issuance and verification of certificates and data associated with the CXC's students, as well as develop the capabilities needed to add new countries into the Regional Blockchain Educational Credentialing solution and to enhance the implementation of CARICOM's free movement of skills.

The certificates and the data should be delivered in a secure way to the students and be able to be presented to universities and employers to be verified in real-time providing that it:

- Mitigates certificates fraud.
- Protects and builds confidence in CXC's e-certificates.
- Allows students to have a digital "wallet" to store their verifiable academic achievements and to allow other institutions to leapfrog the digitalization process.

The solution to be proposed and developed should comply with the following criteria:

- ✓ Have a secure, reliable and traceable solution for issuing, managing and verifying credentials.
- ✓ Verifies that the registration information of the users is valid and proposes methods and procedures for improving data collection.
- ✓ Guarantee the data integrity and control the access to the data.
- ✓ Allow the permanent availability of the information loaded and delivered.
- ✓ Promote the transparency in the exchange of the data associated with certificates.
- ✓ Prove that a certificate presented is genuine and belongs to the holder.
- ✓ Reduce times and costs by guaranteeing an optimal issuance and validation of certificates.
- ✓ Strengthen the veracity of the certificates by ensuring transparency and confidence.
- ✓ Have a visualization mechanism for stakeholder's certificates to access student`s academic records.

This document describes the requirements of Regional Blockchain Educational Credentialing solution that includes the validation of the platform with the 3 countries and stakeholders involved from Barbados, Jamaica and Trinidad y Tobago. The solution proposal should consider scalability as other countries could eventually use the solution, as one of the main characteristics.

5. Scope of the pilot and metrics

5.1. Scope of the pilot

- To develop a platform and an app managed by CXC for issuance, management, presentation and verification of credentials.
- To integrate the platform with CXC ORS system for the issuance of the credentials.
- To be tested with students and entities from 3 countries: Barbados, Jamaica and Trinidad & Tobago.
- To issue certificates CAPE for people over 18.
- To be compatible with parent or supervisor approval, once other certificates are eventually issued to under 18 students (which will not happen as part of the pilot and requires a prior legal assessment by CXC).
- To develop a solution flexible to issue any other type of credential.
- To allow issuing of digital credentials to people that received them in the past, with easy upload of information.
- To validate the registration of information of the students before issuing any credential. The validation mechanisms have to be agreed with CXC.
- The target population are all those students that will be issued or have been issued CAPE certificates and have validated registration information that can be trusted to issue digital credentials. This has to be estimated as the first step of the pilot.
- To deliver a report with the validation mechanisms (for the registration information) and potential improvements in the registration processes and discuss it with 3-5 schools to be implemented.
- To measure how many credentials are issued, accessed via app or platform, shared via app or platform and verified by universities and employees via app or platform.
- To develop an interface to capture feedback from verifiers on the verification of the digital credentials.
- To promote with the verifiers and with the students (the presenters) the use of the digital credentials.

- To develop and carry on a campaign for the dissemination and adoption of the digital credentials.
- To develop a transition and migration plan from paper-based credentials to digital credentials based on each stakeholder needs.

5.2. Metrics

- Number of users with validated registration data to participate in the pilot.
- Number of users that are issued a CAPE credential.
- Number of users that log in via platform or app to access the digital solution.
- Number of presentations of credentials.
- Number of universities and employers that accept the presentation of digital credential (as complementary to the traditional application process).
- Number of credentials that are verified by universities and employers.
- Number of schools that incorporate the recommendations in the on-boarding processes.

6. Technical development per Country[2]

Following the lessons learned during the pre-pilot, the solution to be developed in this new phase to manage the issuance, delivery, and verification of the educational certificates using blockchain should meet the following requirements:

- The solution should be standardized and customizable to leverage blockchain technology for the issuance and verification of a digital academic credential, a CAPE academic credential and future academic credentials that will be eventually issued by CXC and other institutions.
- The solution should consider the scalability requirements, roadmap and action plan needed to add other countries of the Caribbean region.
- The solution should consider the CXC's suite of qualifications examinations[3] for future incorporation and deployment of this modules.
- The firm must develop a suit of lessons learned from the on-boarding and verification processes as part of the deliverables, so it can be applied in some schools and universities.

6.1. Blockchain Components

6.1.1. Users: Natural or legal persons that will have a role in the solution. The actors should be identified by the hired firm, including their roles, permissions, and access to the blockchain. A proposal for the users and their roles is presented in Annex B. The firm must review it, take it into account, make their own proposal and validate it with the stakeholders.

6.1.2. Assets: Assets are the digital representations of physical items that need to be created in the blockchain and can be owned, issued, transferred and stored by the different users. For this project, at least four assets must be created in the form of tokens

[2] Countries participating in this Pilot: Barbados, Jamaica and Trinidad & Tobago.
[3] CXC offers a suite of 6 qualifications examinations: Caribbean Secondary Education Certificate® (CSEC®), Caribbean Primary Exit Assessment™ (CPEA™), Caribbean Certificate of Secondary Level Competence® (CCSLC®), Caribbean Vocational Qualification (CVQ), Caribbean Advanced Proficiency Examination® (CAPE®) and CXC® Associate Degree (CXC®-AD).

that represent digital credentials:

- UsersID: A DID-like identification for any user that signs up in the platform or app.
- StudentID: A DID-like identification for students that will play the rol of their academic digital identity, building a layer of identity on top of their unique identification that allows them to proof to they are, receive, manage and present academic credentials.
- ParentID: A DID-like identification for parents of students under 18 that will play the rol of their academic digital identity, building a layer of identity on top of their unique identification that allows them to proof to they are, receive, manage and authorize the presentation of academic credentials by their children. (This functionality will not be used for the pilot but must be enabled)
- Academic credential: The Verifiable Credential representing an academic title. Must be assigned to a specific StudenID.

Credentials must follow the Verifiable Credential [4] (VC) standard by the W3C. The minimum fields of these credentials should have a detailed review of the attributes to be accomplished with CXC.

The content of the credentials must not be stored in the blockchain. The credentials must only be used to store the proofs of the validity of the credentials. The credentials must be stored in trusted devices and databases owned by the Users and CXC.

6.1.3. Transactions: Transactions are defined as the operations through which participants create, exchange, and modify assets or register any information in the blockchain. It is important to include the validation process as part of the rules.

The system shall assure integrity offering concurrency control over the transactions. At least, it must be possible to:

i. Create credential
ii. Update credential
iii. Revoke credential
iv. Present credential
v. Verify credential

6.2. Academic digital credentials

Academic credentials are digitally represented by the AcademicCredential and are issued to students previously identified by a UserID and a StudentID. Some considerations:

- For the scope of the pilot, academic credentials will only be issued by CXC.
- When students are under 18, credentials can't be managed by the students and must be managed by their parents. There must be two attributes in the credential to identify the student and the parent, and it must not be possible to share or use the credential without the authorization of the parent (via app or platform). This functionality will not be used in

[4] https://www.w3.org/TR/vc-data-model/

this pilot as the scope population will be over 18. However, the functionality will be developed for the solution to be ready to issue credentials to students under 18 when all the legal matters are clear.

- When a user turns 18, they automatically must be able to start presenting and sharing their credential without any authorization of their parents required.
- For users to be able to present academic credentials (mainly to universities they are applying to, and employers they want to work for), practical and secure implementations must be developed. When the credential is presented, there must be two documents that are generated, a readable presentation (ie. a PDF) and a verifiable presentation (ie. a JSON) against the blockchain. For security purposes, both presentations will have an expiration date of two weeks, and need to be signed by the private key of the user that corresponds to the public key of their UserID or ParentID, that can be checked in a Trusted List that must be enabled and owned by CXC.
- Those universities and employers accepting digital credentials, would provide an address to send the presentations to (via app or website).
- The verifiers must be able to view the readable format (PDF), and the website and the app must also enable the verification of the verifiable format (JSON) against the blockchain and Trust Lists.
- CXC will also keep a spreadsheet listing UserIDs, Names, Last Names, Emails, StudentID Public Keys, ParentID Public keys and CredentialIDs associated to them that is connected to the information stored in the blockchain and that can be share to partners for verification.
- There must be a recovery mechanism to retrieve the credentials if the private keys or the credentials themselves are theft or stolen. The recovery must be done through an interaction with CXC. CXC has already a process for re-issuing credentials, so the firm will have to review that process and asses if it this possible to leverage it for retrieval of the digital credentials, or if a new process has to be set.
- The credentials will be stored in the student's wallets and in a CXC database. When the students access the platform via website, the presentation of the credential will be generated from the credential in CXC's database. When they access the solution via app, the presentation will be generated from the credential stored in their app.

6.3. Identification, authentication and authorization

The identification, authentication and authorization of users will be achieved through DIDs[5] and Verifiable Credentials[6]. In order to accomplish that, the credentials described in Section 6.1.2. must be developed. Some considerations:

- The two interfaces to be developed (app and website) as described in Section 6.5 must allow any user to be sign up. This will generate a DID for that user. That is a UserID. A database will be developed to have a record that matches the sign-up information with the DIDs. CXC will own this database.
- When users sign up (or log in fir the first time via app), the primary private keys for the authentication against the DID must be stored in the user app. When they do it via website, there will be a call to a database that matches the log in info with the DID and a proxy smart contract will represent the user at the blockchain level if applicable (i.e.

[5] https://www.w3.org/TR/2019/WD-did-core-20191107/
[6] https://www.w3.org/TR/vc-data-model/

accessing the credentials)

- If the user is a student or a parent, in order to be able to receive academic digital credentials, they need a credential StudentID or a ParentID respectively. The firm to be hired has to review CXC's processes for the validation and verification of the student's identities from their databases. Once an identity is considered validated by CXC and there is an e-mail associated to it, a link via e-mail should be provided for that user to be able to sign up or log in, against the platform or the app, so the user can get their StudentID or PartentID credential associated to that account. For the scope of the pilot, there will not be any issuance of ParentID credentials.
- When the credentials are presented, they must be signed by the public key of the user corresponding to their StudentID or ParentID credential, that play the role of an academic digital identity. The following has to be verified as part of the verification process of the credential:
    - The credential is in a valid format.
    - The credential was issued by a trusted issuer (for the pilot, always CXC).
    - The credential has not expired nor has been revoked by the issuer.
    - The subject of the credential is the same person that is presenting it (or is authorized) because the credential is signed with the StudentID or ParentID of that user.
- It must not be possible for an entity that is not authorized to present that credential to others and pass the verification check, as the credential cannot be signed by someone that is not in possession of the private keys of the StudentID or ParentID.
- CXC will keep a trusted list of StudentID, ParentID and AcademicCredentials playing the role of a CRL.

6.4. Blockchain network/infrastructure

The solution proposed is a hybrid between a permissioned public and a permissioned private network, according to the ISO/TC 307 classification[7]. The network must have the following requirements:

- CXC must have validator nodes (nodes that participate in the consensus protocol) and writer nodes (nodes that generate transactions).
- Ministries of Education and Academics could have writer nodes.
- The writer nodes must be connected both to CXC validator nodes and to LACChain Besu network's[8] validator nodes, so all the information is registered -replicated- in both networks (the private one enabled by CXC's validator nodes and the public one enabled by LACChain's validator nodes) adding redundancy that benefits decentralization and security.
- The vendor must help and assist CXC and the other Users in the deployment of the nodes in the cloud of their preference or on premise.

6.5. User Interface Functionality

A wallet-like app compatible with iOS and Android must be developed for Students and Parents to manage the credentials. A website mobile responsive (the Platform) must be

[7] https://www.iso.org/committee/6266604.html
[8] https://github.com/lacchain/besu-network

developed as well in order for all the other Users to access the system. The wallet-like app would ideally be embedded in the Platform.

This section contains the requirements for the user interface (UI) specific to the scope of the implementation:

- The user interface has to be in English.
- All the information should comply with General Data Protection Regulation (GDPR).
- We will divide these requirements into the seven main profiles, subject to be modified according to the roles and attributes that will define by the vendor in Section 6.1.1.

6.5.1. CXC

a. Registration/ Login
b. CXC Certificates Visualization interface
c. CXC Student's data Visualization interface
   - Integration with the information in the CXC's current systems (i.e. ORS).
   - Verification mechanism and proofs.

6.5.2. Ministry of Education (MOE)

a. Registration/ Login
b. Ministry Interface

6.5.3. Schools (Secondary Schools, Colleges and Universities)

a. Registration/ Login
b. School Interface

6.5.4. Students

a. Registration/ Login
b. Student Interface

6.5.5. Parents/Guardian

a. Registration/ Login
b. Parent/Guardian Interface

6.5.6. Employers

a. Registration/ Login
b. Employer Interface

6.5.7. Accreditation Council

a. Registration/ Login
2. Accreditation Council Interface

6.6. API Development

a. It is required to develop incoming and outgoing APIs for the Platform to interact with the blockchain.
b. Security layers between the app and the node must be developed, as https connections.
c. It is expected the use of standard frameworks as API REST and Open API.
d. API Authentication is required. It is recommended the use of Auth 2.0 with JWT.

7. Key activities

To accomplish the successful development and implementation of the issuance of blockchain credentials by CXC, the pilot will focus on (but not limit itself) to:

i. Coordination of the stakeholders of the pilot identified by CXC.
ii. Digital issuance of credentials.
iii. Verification of credentials.
iv. Validation of student's registration information.
v. Creation of user's academic digital identity.
vi. Validation processes for user's registration data, and enhancements of the registration processes at schools.
vii. Carry out weekly meetings with IDB and CXC team leaders.
viii. Coordinate, lead and carry out workshops with IDB, CXC and key Stakeholders. These can be carried out in person and virtually. At least 1 workshop should be carried out in person in one of the 3 countries.
ix. Carry out in- site training to each country and key stakeholders.
x. Develop the scalability plan needed to add other countries of the Caribbean region. Develop the sustainability plan needed to maintain and scale the solution from an economics and governance perspective.

8. Expected Outcome and Deliverables

To make this project successful, the proposed solution needs to comply with the following requirements:

8.1. Solution Development/Deployment/Validation/Testing:

i. Project Plan and Roadmap
ii. Kick-off meeting/Inception meeting
iii. Solution Design document (proposal and approval) – Including proposed architecture
iv. Prototype and Validation Plan (Front-end Mock-up)
v. Back-end Diagram (Architecture Approval)
vi. Technical Design document
vii. Test Plan
viii. Solution presentation meeting. Location to be determined.

8.2. Training:

ix. Capacity Building Plan– in-site training should be provided (at least 1 per country)
x. User Manual
xi. Admin Manual
xii. Source Code (Application, Smart Contracts, APIs)

8.3. Pilot Campaign:

xiii. Dissemination and adoption campaign
xiv. Transition and migration plan from paper-based credentials to digital credentials
xv. Validation processes for user's registration data, and enhancements of the registration processes at schools.

8.4 Next steps:

xvi. Maintenance and support budget.
xvii. Lessons learned from the on-boarding process
xviii. CXC's manual step by step for future incorporation and deployment of other academic credentialing suites.
xix. Scalability requirements, roadmap and action plan needed to add other countries of the Caribbean region, including budget.

9. Project Schedule and Milestones

Delivery Schedule			
Deliverable			**Date**
Phase 1: Solution Development/ Deployment/ Validation/ Testing	i.	Project Plan and Roadmap	/2020
	ii.	Kick-off meeting/Inception meeting	
	iii.	Solution Design document (proposal and approval) – Including proposed architecture	/2020
	iv.	Prototype and Validation Plan (Front-end Mock-up)	
	v.	Back-end Diagram (Architecture Approval)	
	vi.	Technical Design document	
	vii.	Test Plan	
	viii.	Solution presentation meeting. Location to be determined.	
Phase 2: Training	ix.	Capacity Building Plan– in-site training should be provided (at least 1 per country)	/2020
	x.	User Manual	
	xi.	Admin Manual	
	xii.	Source Code (Application, Smart Contracts, APIs)	
	xiii.	Dissemination and adoption campaign	/2020

Delivery Schedule			
Deliverable			**Date**
Phase 3: Pilot Campaign	xiv.	Transition and migration plan from paper-based credentials to digital credentials	
	xv.	Validation processes for user's registration data, and enhancements of the registration processes at schools.	
Phase 4: Next steps	xvi.	Maintenance and support budget.	/2020
	xvii.	Lessons learned from the on-boarding process	
	xviii.	CXC's manual step by step for future incorporation and deployment of other academic credentialing suites.	
	xix.	Scalability requirements, roadmap and action plan needed to add other countries of the Caribbean region, including budget.	

10. Reporting Requirements

10.1. A progress/fulfillment report detailing the evidence of each of the deliverables shall be presented based on the project schedule in section 8 and section 9.
10.2. All reports should be presented in English, in Word format.
10.3. Supporting materials should be presented in its original format with full usage rights for dissemination (including any presentations, YouTube, social media, graphic material).
10.4. Weekly meetings (either remote/virtual or physically, if possible) should be set up with the Supervision Team (see section 13) for coordination and with the stakeholders for the follow up of the pilot.

11. Acceptance Criteria

11.1. All deliverables shall be considered acceptable once they are presented in full contemplating both CXC and IDB comments, feedback or inputs.
11.2. For the applicants, it is required to present at least (i) a proposal for the communication campaign, (ii) a roadmap for the project, (iii) the working methodology, (iv) the profiles of the people involved, (iv) the experience of the firm and the profiles selected to participate in the project, (v) the architecture diagrams for the different components to be developed, (vi) the blockchain-based solution for the digital identity.

The technological solution shall consider the following points:

i. The solution implementation should start on th, 2020 and end on th, 2021 (x weeks).
ii. Provide a corrective maintenance and support period of 6 months from the acceptance date.

12. Other Technical Requirements

12.1. Type of consultancy: firm

12.2. The firm should have proven knowledge of the region (Caribbean).
12.3. The firm should have proven knowledge of Blockchain technology and regional Blockchain ecosystems such as Alastria and LACChain.
12.4. Experience in project design with digital solutions.
12.5. The firm should have at least a change management leader, a quality manager, and a project manager assigned to the project with 24/ 7 availability.
12.6. Familiarity with regulations, standards and guidelines such as:

- or Electronic Identification, Authentication and Trust Services (eIDAS)
- General Data Protection Regulation (GDPR)
- or Decentralized Identifiers (DIDs)
- or NIST 800-62B (digital Identity)
- or ISO 27001 (information security management) and ISO 24760 (identity management)

13. Supervision and Reporting

13.1. The project will be managed by a project team including the team leader Fernando Yitzack Pavon (fernandop@iadb.org) from SCL/LMK, Mario Casco from (mariocn@iadb.org) and Marcos Allende from ITE/IPS (marcosal@iadb.org)
13.2. Reports of the deliverables shall be presented based on the project schedule in section 7. Comments, approvals or any instructions for changes shall be channeled through the IDB's designated project team members.
13.3. The firm should address IDB's and CXC's concerns/comments/inputs prior to presenting finalized deliverable.

14. Schedule of Payments

14.1. Payment terms will be based on section 6 and section 7. The IDB does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The IDB wishes to receive the most competitive cost proposal for the services described herein.
14.2. The IDB Official Exchange Rate indicated in the RFP will be applied for necessary conversions of local currency payments.
14.3. Payment Consideration should include implementation, licenses and infrastructure costs as part of the proposal.

Payment Schedule			
Deliverable			**%**
Phase 1: Solution Development/ Deployment/ Validation/ Testing	i.	Project Plan and Roadmap	40%
	ii.	Kick-off meeting/Inception meeting	
	iii.	Solution Design document (proposal and approval) – Including proposed architecture	
	iv.	Prototype and Validation Plan (Front-end Mock-up)	
	v.	Back-end Diagram (Architecture Approval)	
	vi.	Technical Design document	

Payment Schedule			
Deliverable			**%**
	vii.	Test Plan	
	viii.	Solution presentation meeting. Location to be determined.	
Phase 2: Training	ix.	Capacity Building Plan– in-site training should be provided (at least 1 per country)	35%
	x.	User Manual	
	xi.	Admin Manual	
	xii.	Source Code (Application, Smart Contracts, APIs)	
Phase 3: Pilot Campaign	xiii.	Dissemination and adoption campaign	10%
	xiv.	Transition and migration plan from paper-based credentials to digital credentials	
	xv.	Validation processes for user's registration data, and enhancements of the registration processes at schools.	
Phase 4: Next steps	xvi.	Maintenance and support budget.	15%
	xvii.	Lessons learned from the on-boarding process	
	xviii.	CXC's manual step by step for future incorporation and deployment of other academic credentialing suites.	
	xix.	Scalability requirements, roadmap and action plan needed to add other countries of the Caribbean region, including budget.	
Total			**100%**

Annex A – Assessment of the Learning Machine Technology (LMT) pre-pilot

The CXC has recognized that digital technology can transform key aspects of how they do business, and the pre-pilot of regional blockchain credentialing was a clear example of that.

The pre-pilot that was initiated by CXC and LMT with the purpose of utilizing a blockchain network and an open-standard digital credential for the issuance of academic credentials. It allowed students to own a digital 'wallet' containing their provable academic credentials.

After an evaluation of the pre-pilot by Ernest and Young (EY), the following conclusions were presented:

The information which underpins the details which follow, were derived from interviews with CXC staff, a meeting with LMT and IDB, a review of LMT website, and an analysis of the CXC/LMT current contract. Various stakeholders were also consulted on their perspective of the solution as it currently pertains.

We have chosen to place the pre-pilot as being between the Proof of Concept and Minimum Viable Product stages, using EY's typical blockchain delivery process shown in Figure 1. In this instance, lessons learned, and feedback become very useful inputs in moving forward. Some of the key findings are summarized as follows:

- The pre-pilot was not constrained to Barbados, Jamaica and Trinidad; but rather covered most of CXC member countries.
- Via email notification (from cxccerts@cxc.org), the pre-pilot made about 115,000 certificates available to students.
- The emails were sent to the email addresses provided by the students during their secondary school examination registration process. Consequently, these email addresses would be an unknown mix of student, parent, or guardian's etc. email addresses.
- There was limited, if any, communication to students at the school level that the email addresses would be utilized for receiving e-certificates. The CXC's communications process appears to be inadequate in this regard.
- At least one Ministry in the three target countries was aware of the blockchain technology pre-pilot but did not effectively communicate the impact of its introduction to their secondary schools.
- The adoption level of the pre-pilot was significantly lower than expected, at about 4.3%. While no number was provided, CXC clearly hoped for a much higher uptake.
- There are several gaps in functionality that need additional components to build out a more robust system, even at the pre-pilot stage.
- Whilst there is a requirement for immutable and secure storage of certification data for third party verification, there is not a strong case for ledger distribution due to the limited number of nodes in the initial implementation.
- The verifier approach could be open to fraud, along with other identity management and trust issues.
- The level of enterprise integration and security appears to be weak even for a pre- pilot e.g., moving candidates' credentialing data between CXC and LMT via email rather than using an API.
- Blockchain distributed ledgers will not resolve inadequate performance issues of the portal on results day – the day on which CXC and CAPE results are released to students - which appears to be a perspective held by key CXC stakeholders.

- The Blockcerts standard is still evolving, and there is a risk that CXC's future need may cause it to deviate from the standard to make it fit their needs (secondary school certificates vs. university).
- The verification journey, which is a fundamental process is easily imitated.
- More thought was expected on identity and access management, and the issues around changing wallet ownership, sharing wallets etc.
- A potential lack of interoperability with other systems or platforms (blockchain or non-blockchain) within CXC and its external stakeholders could impact the capability of the solution going forward.
- There appears to be limited knowledge of the LMT solution within CXC, and a lack of clarity on what exactly was purchased via the 13 August 2018 CXC/LMT Agreement.
- The pre-pilot only provides a vendor specific hash of the certificate – there are possible ways that any certificates could be added via other systems or without using the Learning Machine platform.
- The role of the IT group with CXC was not optimized during the implementation process to maximize knowledge transfer and to develop their internal capability to specify new functionality and to grow the solution to meet the evolving needs of CXC.
- It does not appear that a business case was developed for the LMT solution and therefore it is difficult to judge whether the pre-pilot supports the future requirements of a lifelong learning record and support for the CSME (which is now the subject of this current EY engagement).
- There is limited knowledge within CXC on LMT's solution which could slow any future integration required.
- It is not clear whether the LMT's development roadmap for their product will be consistent and in alignment with the direction of CXC.
- In the absence of appropriate analyses and scenario planning, it is unclear whether the running costs of the LMT solution are sustainable over its lifetime.
- LMT's blockchain based solution solely focuses on certificates and it would be extremely challenging to expand its capabilities to accommodate CXC's requirements in other parts of their business.
- Other non-blockchain components will be needed to support CXC's wider vision.
- Though the hashes of the certificates are deployed on a decentralized data store (the blockchain), the remaining platform is centralized offering universities no option to deploy their own platforms for this.

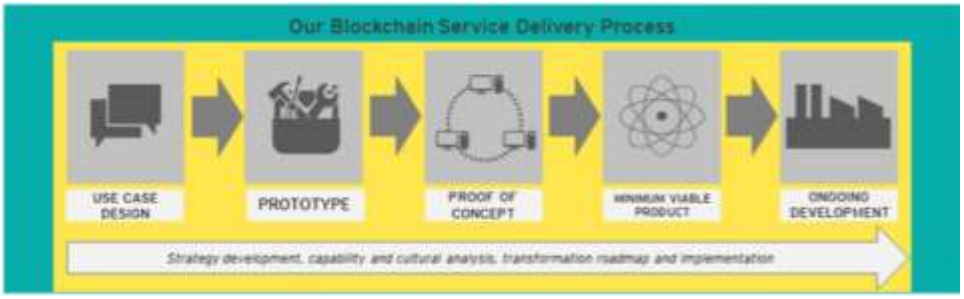

Figure 1: EY's Blockchain Delivery Process

Annex B – Preliminary analysis on blockchain components and user interfaces

This annex presents a proposal for the blockchain components

1. Blockchain Components

1.1. **Users:** Natural or legal persons that will have a role in the solution. As far as the pre-pilot is concerned, the following table specifies the actors that have been identified, including their roles, permissions, and access to the blockchain.

User	Role	Permissions on student's data registration	Permissions on the Certificates	Access to the blockchain
CXC	General Administrator	Read & Write	Read, Write & Verify	Yes
Ministry of Education	User	Read	Read & Verify	Yes
Secondary Schools	Administrator & Validator	Read	Read & Verify	Yes
Colleges or Universities (Higher education)	Administrator & Validator	Read	Read & Verify	Yes
Students Under age	Guest user	Read	Read & Present	No
Students Legal age	User	Read	Read & Present	No
Parents/ Guardian (third party holder)	User	Read	Read & Present	No
Employers (industry bodies)	Validator	Read	Read & Verify	No
Accreditation Council (CSME)	Validator	Read	Read & Verify	No

1.2. **Assets**: Assets are the digital representations of physical items that need to be created in the blockchain and can be owned, issued, transferred and stored by the different users. For this project, at least three assets must be created in the form of tokens that represent digital credentials. The first and second one for identification and authentication, and the third one corresponding to the academic credential. Both credentials must follow the Verifiable Credential [9](VC) standard by the W3C. Below we detail the minimum fields these credentials must have but a detailed review of the attributes must by accomplished with CXC.

The following credentials are a proposal based on the information that has been gathered up to date. The firm hired should take them into account, provide their own proposal, and validate it with the

[9] https://www.w3.org/TR/vc-data-model/

stakeholders from the technical perspective and the business perspective (checking that all the necessary fields are included).

Credential #1 - UserID:

a. DID identifier
b. Type of User (up to 50 alphanumeric characters)
c. Issuer (up to 50 alphanumeric characters)
d. Issuance date (up to 50 alphanumeric characters)
e. Expiration date (up to 50 alphanumeric characters)
f. Verification mechanism and proofs

Credential #2 - StudentID

a. DID identifier
b. Surname (up to 50 alphanumeric characters)
c. First name (up to 100 alphanumeric characters)
d. Address (up to 200 alphanumeric characters)
e. Date of Birth (calendar component for selection of the date and apply the following validation: the date format should be MM/DD/YYYY)
f. Telephone Number (up to 30 numeric characters)
g. Email
h. Gender (incorporate a multiple selection catalog or combo, with the following list: male, female, other)
i. One form of ID (incorporate a multiple selection catalog or combo, with the following list: identification card number, drivers permit number, passport number)
j. Issuer (up to 50 alphanumeric characters)
k. Issuance date (up to 50 alphanumeric characters)
l. Expiration date (up to 50 alphanumeric characters)
m. Verification mechanism and proofs

Credential #3 - ParentID

a. DID identifier
b. Surname (up to 50 alphanumeric characters)
c. First name (up to 100 alphanumeric characters)
d. Address (up to 200 alphanumeric characters)
e. Date of Birth (calendar component for selection of the date and apply the following validation: the date format should be MM/DD/YYYY)
f. Telephone Number (up to 30 numeric characters)
g. Email
h. Gender (incorporate a multiple selection catalog or combo, with the following list: male, female, other)
i. One form of ID (incorporate a multiple selection catalog or combo, with the following list: identification card number, drivers permit number, passport number)
j. Issuer (up to 50 alphanumeric characters)
k. Issuance date (up to 50 alphanumeric characters)
l. Expiration date (up to 50 alphanumeric characters)
m. Verification mechanism and proofs

Credential #4: AcademicCredential

a. DID identifier of the subject
b. DID identifier of the custodian
c. Qualification to be granted
d. Issuer
e. Date of award (up to 50 alphanumeric characters)
f. Issuance date (up to 50 alphanumeric characters)
g. Expiration date (up to 50 alphanumeric characters)
h. Verification mechanism and proofs

The content of the credentials must not be stored in the blockchain. The credentials must only be used to store the proofs of the validity of the credentials. The credentials must be stored in trusted devices and databases owned by the Users.

1.3. Transactions: Transactions are defined as the operations through which participants create, exchange, and modify assets or register any information in the blockchain. It is important to include the validation process as part of the rules. The following functionalities should be included as part of the project and must create a register/transaction in the blockchain when they are executed.

i. Create credential
ii. Update credential
iii. Revoke credential
iv. Present credential
v. Verify credential

The system shall assure integrity offering concurrency control over the transactions.

2. User Interface Functionality

A wallet-like app compatible with iOS and Android must be developed for Students and Parents to manage the credentials. A website mobile responsive (the Platform) must be developed as well in order for all the other Users to access the system. The wallet-like app would ideally be embedded in the Platform.

This section contains the requirements for the user interface (UI) specific to the scope of the implementation. We will divide these requirements into the 7 main profiles based on the roles defined in Section 1.1.

The following flows are a only a proposal. The firm hired should take it into account, provide their own proposal, and validate it with the stakeholders from the technical perspective and the business perspective (checking that all the necessary fields are included).

2.1. CXC

a. Registration/ Login

- The system shall allow administrators to create, update and delete users.
- The system shall allow administrations to invite new users through the institutional and official email with a specific role of those listed in Section 1.1.
- The system shall allow administrations to grant a UserID, a StudentID and a ParentID to the users (for example, via an e-mail invitation).
- Upon receipt of the email, the user will be allowed to register to the system by completing the following fields (some of them might be already identified by CXC so the fields would already be filled):
  - Name (up to 100 alphanumeric characters)
  - Last Name (up to 100 alphanumeric characters)
  - Username (assigned by the system and not subject to be duplicated)
  - Password and Password verification
  - Picture (customizable)
  - Email (up to 100 alphanumeric characters)
  - Telephone (up to 30 numeric characters)
  - Entity name (up to 100 alphanumeric characters)
  - User type (combo selection: Ministry of Education, Secondary School, College, University, Student +16, Student underage, Parent/Guardian, Third party holder, Employers, Accreditation Council)
  - Role. The role will be directly linked with the system's role and permissions as listed in the section 1.1. and must match with the role the invite was issued to.

- Once approved, the person can login using their email or username and password.
- If the user forgets the password, the system will allow the user to change the password by sending a notification to the user with a link to the change password site.
- The system shall allow a user to locate a record through predictive search.
- The system shall send an automatic notification through email to the users, when modifications or updates occur in their data.
- The system shall have an option to read and export analytics reports with the user's information.
- The system shall not allow the duplication of registers and it must be associated to the unique identifier.
- The system shall provide the historic record of the actions taken on every user. (i.e. date of creation, last entry, updates, person who creates the user, etc.)
- The system must keep record of the credentials issued, presented and verified using the app and the website.

b. CXC Certificates Visualization interface

- The system must allow the upload and verification of all the existing certificates from 1979 to present. That upload of information must be done as part of the implementation.
- The system must allow to visualize all the students logged in and sort them by any of the fields, and also to see the certificates associated to them.
- The system will allow predictive search for a specific student or qualification examination.
- The system will allow selecting specific cells and seeing the details of the students.

- The list of students and academic certificates for each of the countries should be available for download as .xls or .csv format through the application.
- The system shall have an option to read and export analytics reports with the historical certificates information of all the CXC country members.

c. CXC Student's data Visualization interface

- Registration of student data or integration with the information in the current systems (i.e. ORS).
- Verification mechanism and proofs.

Notes:

- All the information should comply with General Data Protection Regulation (GDPR).
- The user interface has to be in English.

2.2. Ministry of Education (MOE)

a. Registration/ Login

- MOE representatives shall be invited by CXC via email to the platform including username and password.
- Once the user enters for the first time, the system shall ask the user to enter a new password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.
- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. Ministry Interface

As for the MOE we are planning to provide functionalities to register student's data and validate certificates. Therefore, they should be provided with a dashboard that clearly shows the following:

- Visualization of student's data. (registration student's data)
- Verification of certificates.
- Analytics reports.

2.3. Schools (Secondary Schools, Colleges and Universities)

a. Registration/ Login

- Schools representatives shall be invited by CXC via email to the platform including username and password.
- Once the user enters for the first time, the system shall ask the user to enter a new

password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.
- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. School Interface

As for the Schools we are planning to provide functionalities to register student's data and validate certificates. Therefore, they should be provided with a dashboard that clearly shows the following:

- Visualization of student's data.
- Verification of certificates.
- Analytics reports.

2.4. Students

a. Registration/ Login

- Students shall be invited by CXC via email to the platform including username and password.
- Once the user enters for the first time, the system shall ask the user to enter a new password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.
- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. Student Interface

- Students have to be able to see their student's data
- Students have to be able to see all their certificates.
- Students have to be able to present their certificates in readable (PDF) and verifiable (JSON) format
- Students have to be able to download and print their certificates in readable (PDF) format

2.5. Parents/Guardian

a. Registration/ Login

- Parents shall be invited by CXC via email to the platform including username and password.

- Once the user enters for the first time, the system shall ask the user to enter a new password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.
- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. Parent/Guardian Interface

Parents/guardians have to be able to see all their children´s certificates.

2.6. Employers

a. Registration/ Login

- Employers shall be invited by CXC via email to the platform including username and password.
- Once the user enters for the first time, the system shall ask the user to enter a new password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.
- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. Employer Interface

As for the Employers we are planning to provide functionalities to validate certificates. Therefore, they should be provided with a dashboard that clearly shows the following:

- Verification of certificates.
- Employers have to be able to see the certificates.
- Employers have to be able to download and print the certificates.

2.7. Accreditation Council

a. Registration/ Login

- Accreditation Council shall be invited by CXC via email to the platform including username and password.
- Once the user enters for the first time, the system shall ask the user to enter a new password and verify the password.
- If the user forgets the password, the system will allow the user to change the password by sending an email to the user with a link to the change password site.
- The user will not be able to change their assigned role.

- The users will be able to customize their picture and change their telephone and e-mail. A notification message should be sent to the CXC's administrator and the update of information must be done in the CXC's interface and database.

b. Accreditation Council Interface

As for the Accreditation Council we are planning to provide functionalities to validate student's data and certificates. Therefore, they should be provided with a dashboard that clearly shows the following:

- Visualization of student's data.
- Validation of student's data.
- Validation of certificates.