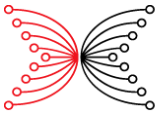

Digital Educational Credential System

White Paper

April 2024

table of content

Executive Summary

The integration of digital credential systems marks a monumental shift in the education landscape, promising to redefine the student journey and revolutionize institutional practices. This white paper encapsulates the multifaceted benefits, challenges addressed, and the holistic transformation that this pioneering step brings to the forefront of education.

By seamlessly integrating digital educational credentials, the transition to higher education is simplified. Cumbersome administrative processes are replaced with efficient digital interactions, allowing students to focus on their academic pursuits. This transformation also empowers students to craft comprehensive digital portfolios that encompass their academic achievements, extracurricular engagements, and skill development. This allows students to have full sovereignty of their data, and share their performance records with third parties of their choice. This digital archive not only celebrates their growth but equips them with tangible evidence of their journey.

With the integration of universities into the digital credential ecosystem, a harmonious network of learning institutions will emerge. This interconnected approach transcends geographical boundaries and aligns recognition standards, making it easier for students to navigate diverse educational paths. The collaboration of universities within this digital framework creates a foundation for standardized recognition and cross-institutional partnerships, propelling education into a new era of connectivity.

The **Digital Educational Credential System** developed by IOG addresses critical challenges faced by educational institutions globally. Administrative processes are streamlined, saving valuable time and resources, which can then be directed toward innovative learning experiences. This digital transformation fosters an environment of trust and authenticity, as credentials are securely stored, thanks to blockchain technology, drastically reducing the risk of fraud. Moreover, the enhanced efficiency and skilled graduates—armed with comprehensive digital portfolios—contributes to the growth of the digital economy, ultimately driving employment opportunities and economic prosperity.

This offering is more than a technological advancement, it embodies a paradigm shift in education. It aligns with the demands of a digital age, offering students a clear and empowered path forward. The result is a harmonious blend of seamless transitions, enriched educational experiences, and robust economic growth, all shaping a future where learning transcends boundaries and potential is boundless.

This white paper describes the **Digital Educational Credential System - a** solution developed by Input Output Global (IOG) and implemented for the Ethiopian Ministry of Education using the Atala PRISM platform.

1. Introduction

1.1. Overview of Digital Educational Credential System

In its publication "Student Information System Market Report, 2022-2030", the United Nations Educational, Scientific, and Cultural Organization (UNESCO) has summarized the challenges faced by educational institutions worldwide. Some of the most significant facts can be summarized below :

- **53%** of institutions rely on **paper-based systems** worldwide, and are not able to consolidate reports at national level
- **36% only** use **student IDs** to manage, plan, and monitor performance
- **29%** of education ministries are **unable to locate schools** they manage, and **even less** able to identify their **performance**

As a result, it appears that more than 50% of education achievements presented by students are fake.

Managing student records in Ethiopia is a complex and challenging task, with significant administrative and logistical difficulties. The paper-based system, with records fragmented across various institutions, made it difficult for the educational authorities to verify credentials and monitor attendance accurately.

The Ministry of Education in Ethiopia aimed to address these challenges by **building a digital system anchored on blockchain-based digital IDs** for students, teachers, and school leaders.

The system aims to **digitize student records via verifiable credentials, improve attendance monitoring, enable frictionless records sharing, reduce fake certificates, and unlock data analytics for policy insights.**

The digital system provides a **secure** and decentralized way to manage student records, enabling students to have full control over their records,allowing them to share their records with authorized parties transparently.

The system also provides a **tamper-proof way to verify the authenticity of credentials,** reducing the risk of fake certificates to make it easier for employers and higher education institutions to verify a student's credentials.

The system enables students to have a digital wallet that stores their verifiable credentials, including academic achievements, certificates, and attendance records. The digital wallet is accessible via a mobile app, enabling students to access their records anytime, anywhere.

The system also enables teachers to record attendance electronically, making it easier to monitor absenteeism in order to support students who may need additional support.

Moreover, the system enables **frictionless records sharing**, making it easier for students to transfer their records between schools and universities. This reduces the administrative burden on students and institutions, making it easier to manage student records and support student mobility.

The system also **unlocks data analytics**. By digitizing student records, the Ministry of Education has access to a wealth of data that can be analyzed to identify trends and patterns in student performance.

1.2. Importance of Verifiable Credentials in Educational Institutions

The correctness and integrity of academic credentials are extremely important for the education sector. Digital records that may be shared securely—and only to authorized parties—are tamper-proof, and can be easily validated are known as verifiable credentials. Verifiable credentials are a crucial element in making sure that academic records in educational institutions are secure and reliable.

Verifiable credentials offer a contemporary and effective solution to manage and certify academic records, especially as technology is used in education more and more. They enable schools to efficiently issue, administer, and validate academic records by offering a secure and transparent mechanism to record students' accomplishments. Credentials that can be verified are also less vulnerable to fraud because they cannot be altered, and therefore, lower the risk of fraud in the educational industry.

Verifiable credentials are essential for maintaining the reliability and accuracy of academic credentials in educational institutions. They provide a cutting-edge and effective method for maintaining and authenticating academic records, boosting public confidence in the educational system, and enhancing prospects for students.

2. Glossary of Key Terms

- **Accessibility:** The degree to which educational resources, tools, and environments are designed to be usable and inclusive for individuals with disabilities.
- **Artificial intelligence (AI):** The simulation of human intelligence processes by computers, including learning, reasoning, and problem-solving.
- **Attendance monitoring:** The process of electronically recording student attendance, which enables educational institutions to report absenteeism, identify patterns, and provide necessary support to students.
- **Background checks:** Verification processes conducted by employers to assess the suitability of a candidate for a particular role or position.
- **Background references:** Online sources and documents that provide additional information, context, or research related to the subject matter.
- **Biometric authentication:** The use of unique physiological or behavioral traits, such as fingerprints or facial recognition, to verify a person's identity electronically.
- **Biometric data:** Unique physiological or behavioral characteristics, such as fingerprints, facial features, or iris patterns, used for identification and authentication.
- **Blockchain protocols:** Sets of rules and standards that govern how data is stored, verified, and shared within a blockchain network**.**
- **Blockchain technology:** A distributed and secure digital ledger technology that ensures the integrity and immutability of data. In the context of the Educational Digital ID System, it is used to provide a tamper-proof and trustworthy verification mechanism.
- **Collaborative efforts:** Cooperative and coordinated actions taken by multiple individuals or entities to achieve a common goal.
- **Curriculum:** The set of courses, subjects, and educational content offered by an institution to support learning and skill development.
- **Data analytics:** The practice of analyzing and interpreting data to extract valuable insights and trends. In the context of the education sector, data

analytics is used to make informed policy decisions and improve student outcomes.

- **Decentralized Identifier (DID):** A new type of identifier that is designed to enable self-sovereign identity on the internet. A DID is a unique, persistent, and globally resolvable identifier that is created and controlled by the subject of the identifier, typically an individual. Unlike traditional identifiers, such as usernames or email addresses, which are often issued and managed by centralized authorities, DIDs are decentralized and can be managed independently by the entity they represent. This allows students to maintain full control of their own data, while giving permissioned access to any administrative systems.
- **Digital divide:** The gap between individuals or communities with access to modern digital technology and those without, often resulting in disparities in educational opportunities.
- **Digital literacy:** The ability to use digital technology effectively and responsibly to access, evaluate, and communicate information.
- **Digital transformation:** The comprehensive integration of digital technology into various aspects of an organization or sector to fundamentally change how it operates and delivers value.
- **Digital wallet:** A secure digital storage system for verifiable credentials, allowing students to access and share their academic records using a mobile app.
- **Economic impact:** The influence of the educational digital ID system on financial aspects, including cost reduction, efficiency enhancement, and economic development within the Education sector.
- **Educational attainment:** The level of education an individual has completed, often measured by degrees, certificates, or qualifications.
- **Educational Digital ID System:** A technology-driven solution aimed at digitizing student records, leveraging verifiable credentials and blockchain-based digital IDs for students, teachers, and school leaders in educational institutions. This system aims to streamline administrative processes, enhance security, and improve data analytics.
- **Efficiency:** The ability to achieve desired outcomes with minimal waste of resources, time, or effort.
- **Entrepreneurship and innovation:** The process of starting new ventures or creating novel solutions, products, or services that contribute to economic growth and development.

- **Financial inclusion:** Providing access to financial services and resources to individuals who are traditionally underserved or excluded from the mainstream financial system.
- **Frictionless records sharing:** The seamless and efficient exchange of student records between Educational institutions with student permission, enabled by digital technology. This reduces administrative burdens and supports student mobility.
- **Google Guice:** Open source software framework for Java platform
- **Global economy development:** The growth and expansion of economies on a global scale, influenced by factors such as trade, technology, and innovation.
- **Higher education:** Post-secondary education typically offered by universities, colleges, and institutions beyond high school.
- **Inclusivity:** Ensuring that all students, regardless of their socioeconomic status or background, have equal access to educational resources and opportunities.
- **Institutional viability:** The ability of an educational institution to maintain its operations, relevance, and success over an extended period.
- **Knowledge sharing:** The exchange and dissemination of information, expertise, and insights among individuals or groups to enhance understanding and decision-making.
- **Logistical overhead:** The operational burden and costs associated with managing physical resources, materials, and processes.
- **Machine learning:** A subset of artificial intelligence (AI) that involves algorithms and statistical models enabling computers to learn from and make predictions or decisions based on data.
- **Merkle tree hash:** In cryptography and computer science, a hash tree or Merkle tree is a tree in which every "leaf" is labeled with the cryptographic hash of a data block, and every node that is not a leaf is labeled with the cryptographic hash of the labels of its child nodes.
- **Micro certificates:** Small credentials or certifications that validate specific skills or competencies, often obtained through short courses or workshops.
- **Paperless system:** An approach that eliminates or significantly reduces the use of physical paper and replaces it with digital alternatives.
- **Personalization:** Tailoring educational experiences, content, and support to individual students' needs, preferences, and learning styles.
- **Policy decisions:** Choices and actions taken by policymakers based on research, analysis, and evaluation of various options and potential outcomes.

- **Policy insights:** Informed decisions made by educational policymakers based on data analysis and trends derived from digitized student records, with the goal of improving educational outcomes.
- **Predictive analytics:** The use of data analysis and statistical algorithms to forecast future trends, behaviors, or outcomes.
- **Prospects for social mobility:** Opportunities for individuals to improve their social and economic status, often through access to education and career advancement.
- **Public confidence:** Trust and belief in the effectiveness, reliability, and credibility of public institutions and systems.
- **Reputation:** The perception and assessment of an institution's credibility, trustworthiness, and standing within its community and the broader society.
- **Software as a Service (SaaS):** Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet.
- **Security breach:** Unauthorized access or exposure of sensitive data, potentially leading to identity theft, fraud, or other malicious activities.
- **Self-Sovereign Identity (SSI):** Refers to a concept and a set of principles that empower individuals with greater control over their digital identities. Self-sovereign identity aims to enable individuals to assert and manage their own identities without the need for centralized authorities or intermediaries. This concept is closely related to the field of decentralized identity and is often associated with emerging technologies like blockchain.
- **Stakeholders:** Individuals, groups, or organizations with an interest in or influence over a particular project, system, or initiative.
- **Strategic imperative:** A crucial and essential action or decision that aligns with an organization's long-term goals and success.
- **Sustainable future:** A vision of the future that prioritizes environmental, social, and economic sustainability, often achieved through responsible practices and technologies.
- **Tamper-proof verification:** The use of technology, such as blockchain, to ensure the authenticity and integrity of academic credentials, reducing the risk of fake certificates.
- **Verifiable credentials:** Digital records that securely and transparently convey academic achievements, certificates, and attendance records. These credentials are tamper-proof, easily shareable, and offer a reliable way to validate academic records.


INPUT | OUTPUT

3. Benefits of Digital Educational Credential System

Digitizing student attainments has its benefits, along with the other digitizing efforts around the globe, in comparison to manual and paper-based systems. The usual benefits are ease of access, speed of sharing, and durability. The institution issuing credentials to students issues them instantly and the students get them simultaneously in their wallet, accessed via the mobile app.

When students want to share their credentials with employers, or other stakeholders like banks, insurance companies, or other educational institutions, they can do so instantly from their phone or laptop.

Students do not need to go to the school registrar to request a certified stamped physical copy, meaning they do not need to personally take the physical copy to the requestor or verifier. They also no longer need to share their personal information with requestors over email.

All students need to do is share their credentials with the verifier, who gets confirmation of authenticity through the verification portal. Issuing the credential on blockchain even has further benefits as explained below in the current document.

Image_01: Institutional hierarchy

3.1. Verifiability, Immutability, and Tamper proofness

3.1.1 Verifiability

Credentials issued to the Cardano blockchain can be verified by anyone as a legitimate credential issued by the issuer. The issuing institution, or a school which is endorsed by the issuing instiution, can be confirmed through the verification process. Hence verifiers have trust in the authenticity of the credential claims by the holders of the credential.

3.1.2 Immutability

There is no risk of losing one's credential after it is issued on the blockchain. In the solution described in the current document, the hashes of the credentials get written to the blockchain, which is used in turn to verify the actual credentials. It does not require a back up as the blockchain ledger is copied around the world. It is also available all the time without depending on any specific client or enterprise infrastructure.
Immutability includes the fact that a VC cannot be reassigned to another individual, making the certificate specific to one identity. This is in contrast with an NFT, which can be reassigned to someone else.

3.1.3 Tamper-proof

Unlike legacy databases where records can be modified, altered, or deleted, records registered on the blockchain can not be modified or deleted due to the very nature of blockchain. Therefore once issued, the verifier is assured it has never been altered in any form since the first issuance and can never be altered afterwards either.

3.2. Streamlined Enrollment and Registration Processes

In the solution described in this document, student registration can be done in person through the current system, or alternatively through a national ID system

(NID), as part of the program's 'Know Your Customer' (KYC) requirements. The student presents their eighth grade passing credentials (which has the full name of the student, date of birth, the photo of the student, his/her results and other information) for registering for ninth grade. For grades 10-12 students present their report from the prior year, and again the KYC is done via the grade report or eighth grade credentials. Upon completion of KYC, the student is provided with an invitation code and url of the system to activate his/her account. Activating his/her account provides him/her with the DID of a holder by Atala PRISM. This DID is used to issue a transcript that is published on the Cardano blockchain as a Merkle tree hash.

3.3. Data Analytics and Insights for Educational Improvements

Data analytics and insights from the system are essential for the overall improvement of the education system. By providing educators and policymakers with detailed information on student performance, and other key metrics, data analytics help drive improvements in educational outcomes and ensure that all students have access to high-quality education. In the solution described in this document, implementation, data analytics and insights are provided from the DID system at various levels, including the issuing institution, the region, and school levels.

3.3.1 Issuing Instiution Report

This report allows the issuing instiution to gain valuable insights into the overall performance of the education system in the country and identify areas for improvement. By analyzing data on user activity within the system, the issuing institutionidentifies trends and patterns in user behavior, institution registration status, insights into student registration, student performance, and insights into teachers and school leaders. The report also provides detailed information on student performance, allowing the issuing instiution to identify schools or regions that may require additional support. Overall, this report is a valuable tool for the issuing instiution in its efforts to improve educational outcomes.

3.3.2 Regional level report

Data analytics provide insights into regional differences in educational outcomes and help identify areas for improvement. This report is similar to the issuing instiution level report but the insight focuses on students, teachers, institutions, and users that exist in the region. It also provides more detailed information about local educational outcomes and helps identify specific schools or areas that may require additional support.

3.3.3 School level report:

This report allows school administrators and leaders to gain valuable insights into the performance of their school and identify areas for improvement. The report also provides detailed information on student academic performance, allowing teachers to identify areas where students may need additional support. Overall, this report is a valuable tool for schools in their efforts to improve educational outcomes.

3.3.4 Examination Agency report

An Examination Agency report on the national exam level provides valuable insights into the performance of students who have taken the exam. The report includes information on the number of students who took the exam, their overall performance, and the overall results of the exam and students' achievement. It also provides a breakdown of student performance by subject, gender, region, or other relevant categories. Additionally, the report includes information on the performance of educational institutions at the country level, such as the average scores of students from different schools or regions. This information is used by educators, policymakers, and other stakeholders to evaluate the effectiveness of educational programs and policies, and to identify areas for improvement.

4. Implementation and Integration

The issuing instiution may implement the system on-premises, comprising all necessary system components. These include a backend service, front-end user interfaces, and nodes to support the Atala PRISM and Cardano blockchain networks. The entire cluster is deployed within the issuing instiution's private virtualized cloud infrastructure, allowing the system to be managed and operated internally.

The system is accessible via the issuing instiution's intranet, for the 3,500 schools; however, institutions that are not part of intranet may access the system over the internet.

4.1 Architecture and Key Components

The IOG DID system may be externally available through two platforms: the Web portal and the Android application.

In addition to these two outlets, there is a reporting API (Application Programming Interfaces) which converts stored and processed data into Excel-based, PowerBI, or RShiny dashboard-based reports that are consumed by the issuing instiution, entities below the issuing instiution, and schools.

The system level hierarchical interaction is done in a highly flexible manner, and considers all the existing and possible cross interactions between the existing hierarchies. The overall hierarchical structure of the solution is displayed in the diagram above.

The system has three primary groups of users interacting through two interfaces (mobile and web). These groups are: students, teachers, and administrators of each level of the hierarchical entities. Architecture and components of each of the interfaces are listed below.

4.1.1 Front-end

The front-end is the main interaction point between the various users and the backend applications for institution creation, staff creation, student registration. It is also the interface point where students' grades are entered, and transcripts are issued.

4.1.1.1 Front-end architectural structure

The front-end application is built using Next.js, a react-based web application framework with server-side rendering and static website generation. Antd (a popular react UI component library) is used by SaaS to build interfaces that enhance user experience.
The entire front-end application is designed to be modular and scalable using Atomic Design philosophy (atoms, molecules, organisms and pages). Custom hooks are used to provide cryptographic and SSI functionalities. Components and modules are separated clearly and injected with mocks to perform unit and integration testing.

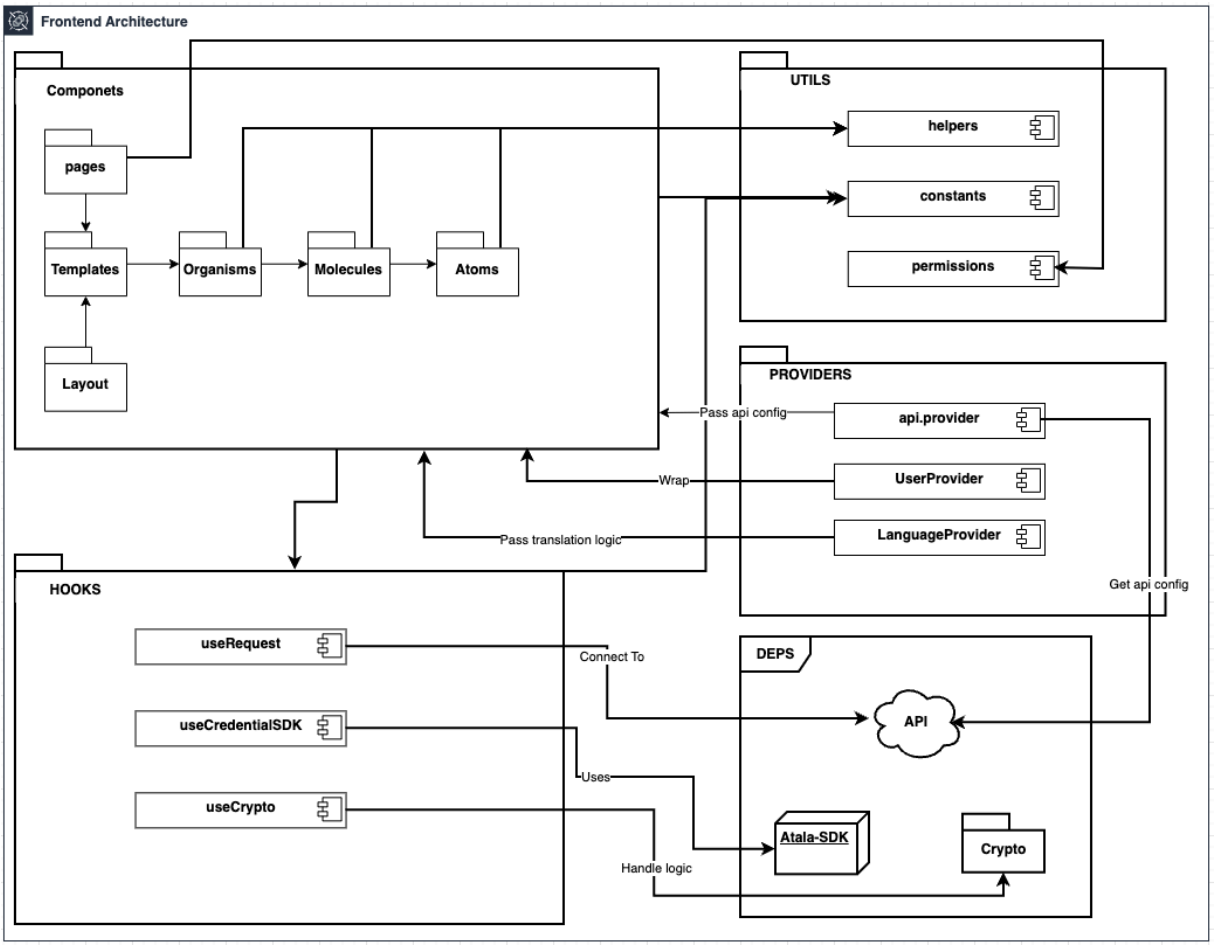

Image_02: Frontend architecture

4.1.1.2 Front-end component flows

These are React components organized using the Atomic Design philosophy. Atoms are the smallest building blocks, usually representing a single component in the user interface like a button or an input field. These components are highly customizable to allow reusability.

The molecules are formed by the combination of more than one atom, a good example is an input field with a submit button. These components are reused to some extent and have less customizability compared to atoms. The organisms at the next level of abstraction are built by the combination of molecules and atoms. As an example, an entire

registration or sign up form as an organism. These components are rarely reused, and are hard to make them customizable.

The pages and layouts are React components that are required by the Next.js framework. They basically represent the routes and web pages.

- **Utils:**

  Utils is a collection of reusable Javascript functionalities used in the application. This module collects many different classes and functions to solve common problems like permission, file, formatters, calendar, etc. These components are separate and tested independently.

- **Providers:**

  React context APIis used to manage state in the application. In this module state providers manage user data, language preferences, global API instance, and more.

- **Deps/services:**

  A module is being used with implementation logic to perform API requests, cryptographic functions and PRISM SDK interactions. These modules are used by many higher level components and are the core of many use cases.

- **Hooks:**

  Multiple custom hooks are used in React components. These modules expose Deps/Service functionalities that are easy-to-use in the components. These functionalities include cryptographic and SSI functionalities.

4.1.1.3 Use Case: Issue a Holder Credential

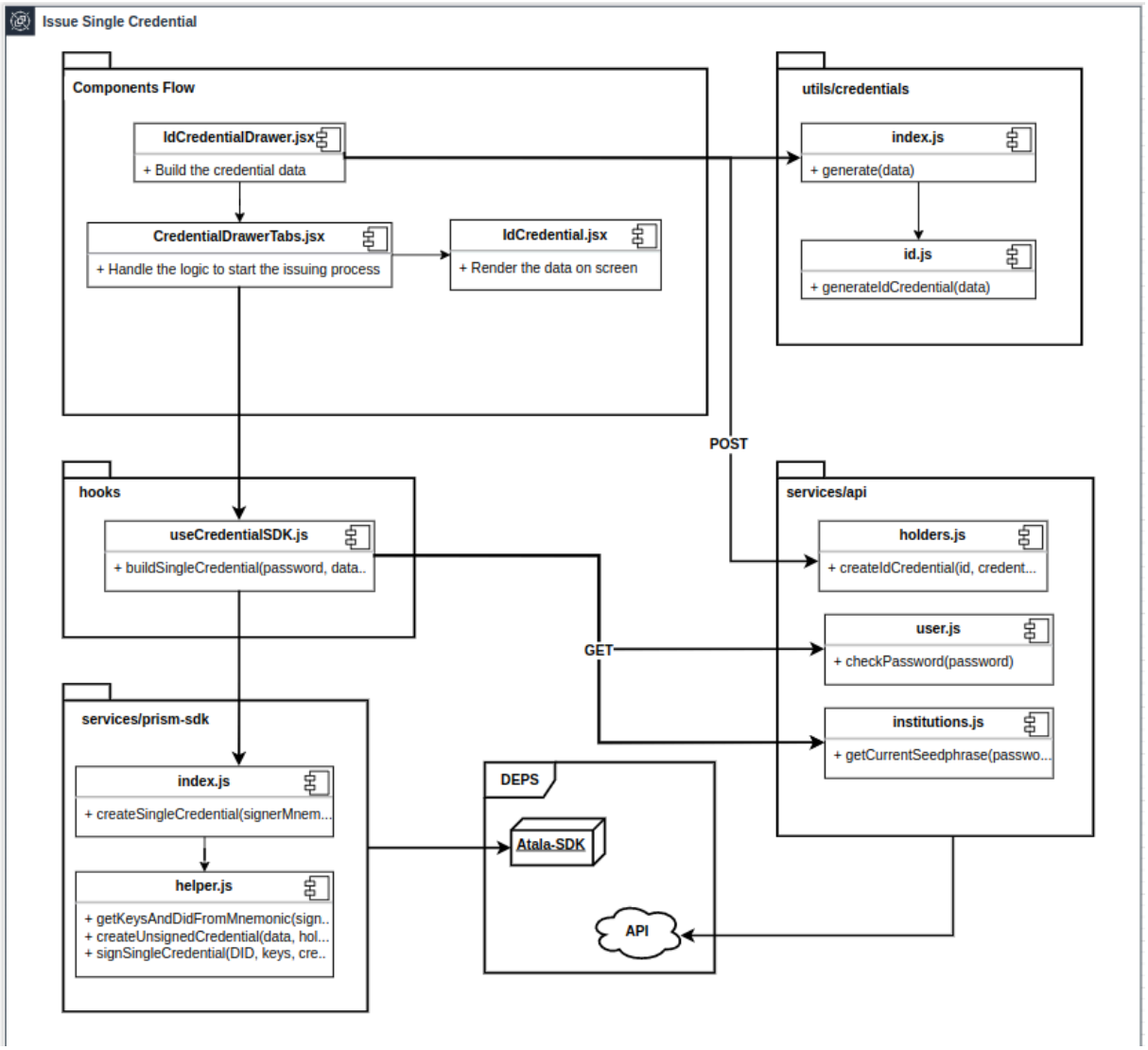

Image_3: Usecase issue a single credential

- **Components flow**

The UI components IdCredentialDrawer, CredentialDrawer, and IDCredential are integral parts of the credential issuing process. IdCredentialDrawer acts as the main user interface, facilitating the rendering and management of ID credentials. It utilizes the CredentialDrawer component to display a drawer interface for interacting

with credentials. ID credential component, on the other hand, handles the rendering of the actual ID credential content. Together, these components enable users to view, create, and revoke credentials while ensuring a seamless user experience.

- **Utils/credential**

The Utils/Credential module is crucial for managing and structuring credential data. It offers functions and utilities to create and format credential information effectively. One of its key functions is generating a structured ID credential object that contains vital details for the credentialing process. This module establishes a reliable framework for representing credentials, ensuring consistent handling and organization of credential data. By leveraging the Utils/Credential module, developers easily work with credential information and ensure its integrity and usability throughout their application.

- **Hooks/useCredentialSDK**

The useCredentialSDK module acts as a bridge between React components and the PRISM SDK. It validates whether a user issues a credential by leveraging the SDK's capabilities. This module streamlines the process of checking user permissions and integrates seamlessly with React components, enabling efficient credential issuance.

- **Services/PRISM-SDK**

The services/PRISM-sdk module utilizes the Atala PRISM SDK to generate the payload of the newly signed credential. This module leverages the capabilities of the Atala PRISM SDK to handle the encryption, signing, and formatting of the credential data. By utilizing this module, the application securely generates the payload of the credential that is stored in the DB so it is verified against Atala later.

4.1.2. Mobile application

The mobile app helps to hold credentials, view credentials, view class results, and schedules for students. The Android app is built using Kotlin programming

language and to facilitate ease of interaction to decentralized identity, Kotlin Atala PRISM SDK is used.

The application follows MVVM architecture with three main layers: data, domain, and presentation, providing separation of concerns, reusability, modularization, and loose coupling. This ensures code reusability, ease of testing, scalability, and maintainability.

4.1.2.1 Mobile application architecture

- **The data layer**

  Is a layer where all data sources are contained. It is a bridge between the application and the system for data operations. There are multiple data sources in the application, network source, local database, and data store. Their responsibilities are:
  - Exposing data to the rest of the app
  - Centralizing changes to the data
  - Resolving conflicts between multiple data sources
  - Abstracting source of data from the rest of the app
  - Containing business logic

- **The domain layer**

Is the business layer that encapsulates the business or domain logic and data. They are collections of entity objects and related business logic that are designed to represent the business model. This consists of model repositories and use cases.

- **Model:** A framework of independent classes that hold data and are used to transfer information in the app.

- **Use cases:** A potential functionality or business logic unit is called a use case. They are functions (classes with a single public method) which contain logic. Use cases perform single operation and they typically combine or transform data from repository or other use cases.

- **Repository:** Mediates between domain and data-source. It maps data into domain models, so that the domain layer only needs to deal with the domain models for business logic.

- **The Presentation layer:**

  Contains components that are related to user inputs and view updates. It includes activities, fragments, viewmodels, adapters, etc.
  A single activity approach is used, where all fragments are hosted in one single activity.

4.1.3 Backend

4.1.3.1 Backend architectural structure and component flows.

Even though the application is based on the Play framework and has a layered architecture, due to the relevance of the application at the initial moment, the decision was made for a package distribution using a Domain Driven Design or Onion Architecture approach in order to have better usability maintenance in the future.

A conventional setup of the Play Framework can be adopted, leveraging the powerful Typesafe Config library and utilizing the HOCON format. This configuration enables an efficient structure and more organized configurations.

Security and game settings are used in a conventional way. In addition to the general ErrorHandler and Module components with Google Guice; however, the application structure was modified to have three layers: infrastructure, application, and domain, as shown in the following diagram:

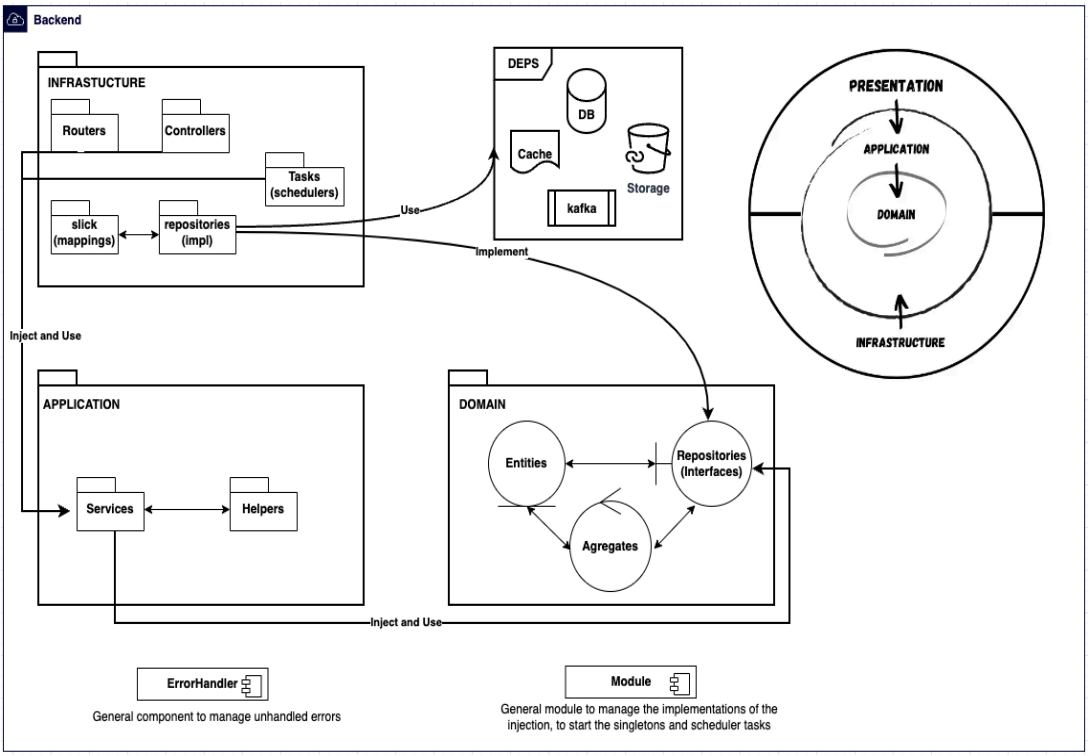

Image_04: Backend Architecture

- **Infrastructure layer:**

It is the outermost layer of the architecture, with multiple objectives. It acts with the routes and controllers as an entry point of the application, while having all the implementation of the domain repository interfaces. It integrates with the defined technology (known as infrastructure adapters), such as Slick for database access, Kafka to handle events, Redis for cache access, JWT for token management, etc.

- **Application layer:**

Where the application services, casually called "use cases", are in charge of orchestrating the steps to correctly handle the requests, and interact with other services and with the domain layer repositories. In addition, it must persist records in the logs of each step that is done to achieve the use case.

- **Domain layer:**

This is the core of the application, encompassing the entities, aggregates, and their behaviors, along with the repositories (without implementation). These components are orchestrated by the application services to cater to each specific use case.

4.1.3.2 Use Case: Issue a Holder Credential

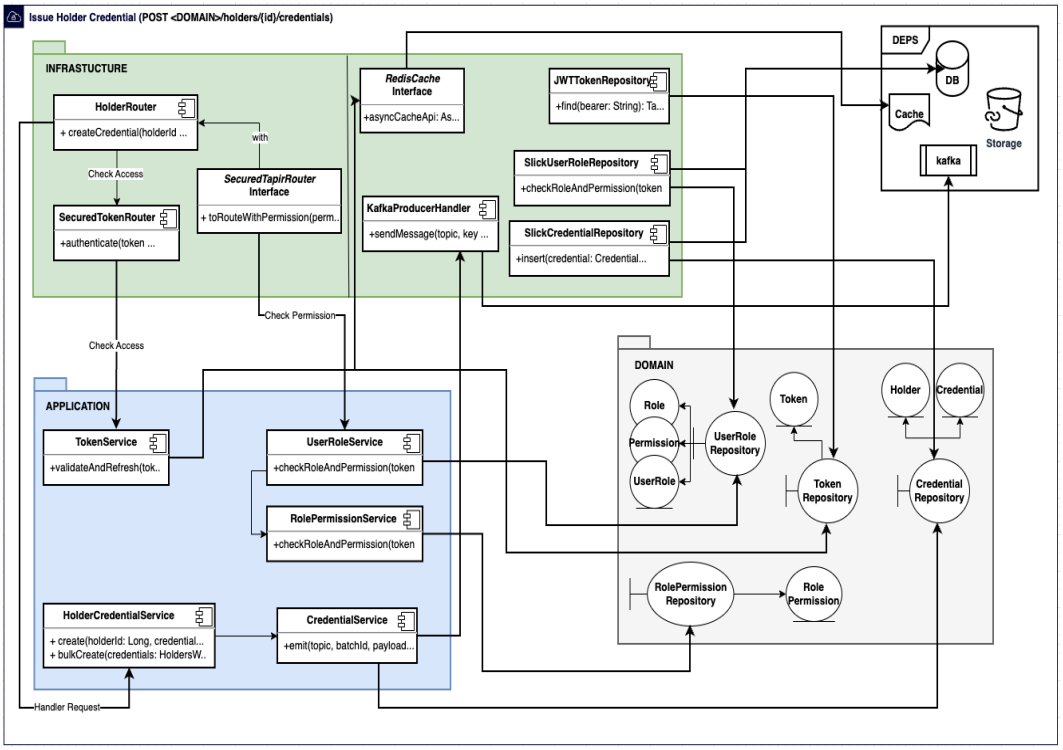

Image_05: Usecase issue a Holder Credential

- **Infrastructure layer:**

Here is the entry point of the use case that handles the POST endpoint to issue credentials. Since it is a secure endpoint, it implements the SecuredTapirRoute interface, which requires injecting the SecuredTokenRouter that includes the authenticate method to verify if the requesting user is authenticated. Additionally, it includes useful methods for checking permissions for each type of operation. In this layer, the Data Transfer Objects (DTOs) are found, which are basically the objects received and returned in the requests, with their respective formats for JSON encoding and decoding.

Additionally, it includes the implementation of domain repositories, which are responsible for interacting with the database. It also has connector helpers for caching, as well as producers and consumers for sending messages to Kafka, as shown in the image on the right side.

- **Application layer**

Here the services responsible for managing all the permissions and validations for logged-in users are found. These services also handle the steps of each use case. For example, in the HolderCredentialService and CredentialService, necessary validations are applied to the holder's status and the executing admin. Additionally, a credential is created in the database, and a message is sent to Kafka with the necessary data to issue the credential on the blockchain through the DID-Service API, and Atala PRISM SDK.

- **Domain layer**

This is the core of the application where all the entities and their behaviors are observed, as well as the repository interfaces that declare each functionality. For instance, repositories and entities are found to be related to access token validation and user roles. However, in the context of this particular use case, it is more significant to focus on the Holder entity. It undergoes a state change once the Credential ID is created. Additionally, the credential entity is inserted into the database to persist all the necessary data through CredentialRepository, which is subsequently updated as other parties interact with the blockchain.

4.1.4. DID service

The DID service handles all tasks related to DIDs and digital verifiable credentials (VCs). Creation, modification, deactivation of DIDs and verification are the services that interact with Atala PRISM.

4.1.4.1 DID service architectural structure and component flows

In this relatively small application, a conventional approach can be adopted by employing modular packaging for each module, such as the DID, credential, and operation modules to effectively manage the outcomes of operations. Additionally, the Atala module can be utilized to facilitate interactions with the blockchain. As mentioned earlier on the backend components, there is the ErrorHandler and Module components, as depicted in the following image:

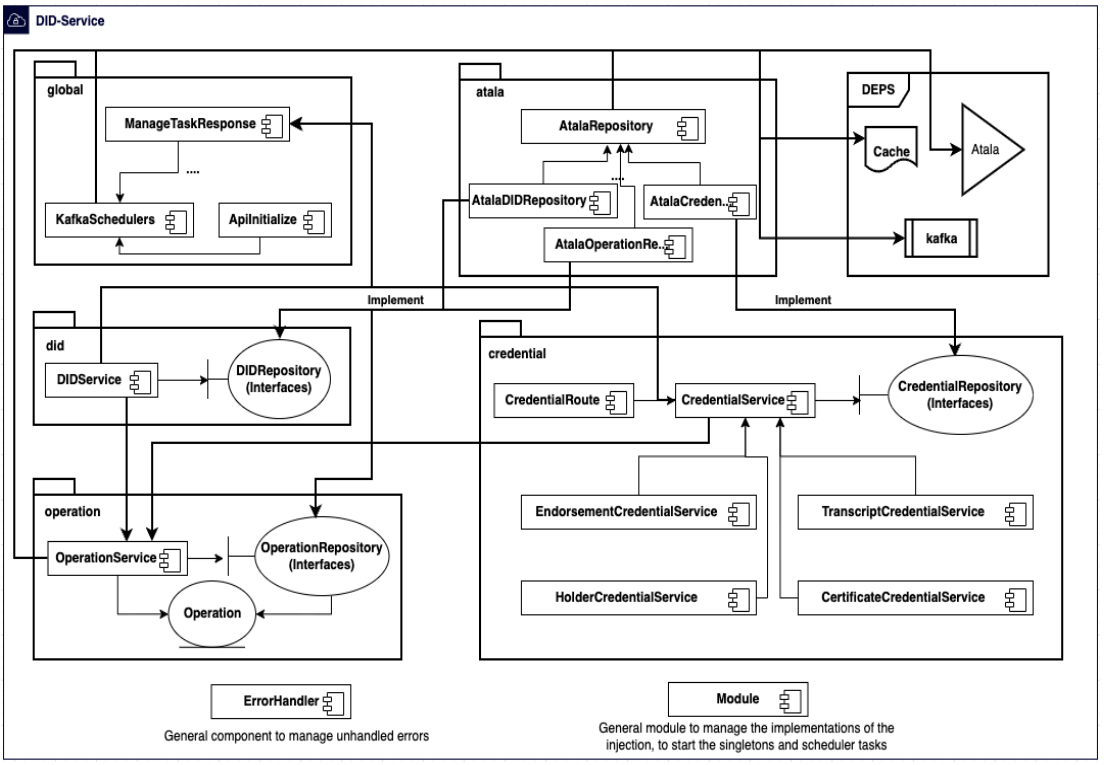

Image_06: DID service

- **Global module:**

The global module stores all the necessary components to boot the application, manage scheduler tasks, Redis, and Kafka. Additionally, it includes some shared classes that are used across all services.

- **DID, credential, and operation modules:**

The DID, credential, and operation modules have the entities, services, and repositories (without implementation) required for the use cases based on the type of operation in the blockchain.

- **Atala module:**

The Atala module encompasses all the implementations of the DID, credential, and operation repositories. In addition, it includes a centralized repository that initializes the Atala PRISM NodeAsync and interacts with the blockchain. This setup facilitates response mocking in test flows

4.1.4.2 Use Case: Issue a Holder Credential

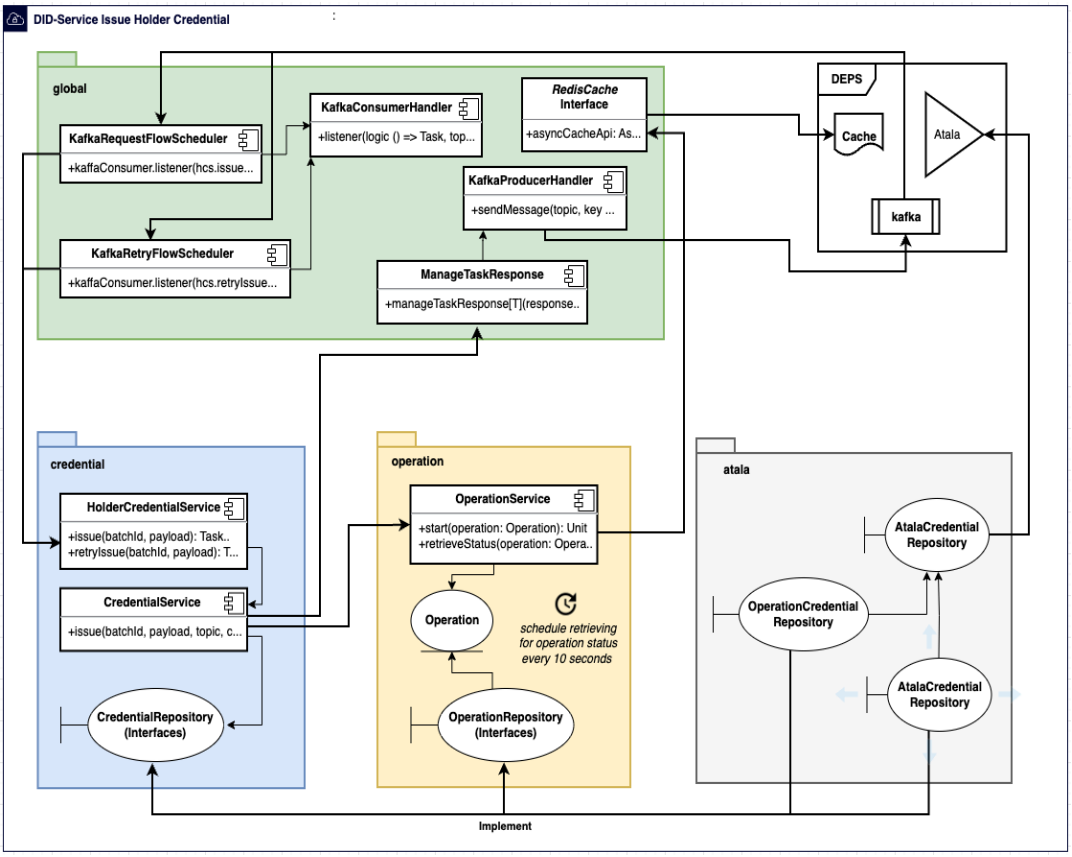

Image_07: DID service Holder credential

- **Global module within the use case**

In this module, there are all the common components of the application that are used by other modules. Additionally, there are Kafka schedulers to handle requests and retry topics (KafkaRequestFlowScheduler and KafkaRetryFlowScheduler). These are capable of initiating a complete flow to the corresponding service from Kafka topic messages.

- **Credential module:**

In this module, all the components related to credentials can be found. For example, the HolderCredentialService is used, which eventually uses the CredentialService, and then, it injects the CredentialRepository, which contains the declarations of the issue, revoke, and verify functions. In this case, the issue function is being used.

- **Operation module:**

The operation module provides an agnostic implementation for all operations using the Atala Operation object, whether it is related to credentials or DIDs. Within the OperationService, a scheduler is started every 10 seconds to check the status of the operation against Atala PRISM using the getStatus method of the OperationRepository.

- **Atala module:**

In this module, all the previously mentioned repositories are implemented using AtalaOperationRepository and AtalaCredentialRepository. All of these invoke AtalaRepository, which serves as the only gateway to the blockchain through the Atala PRISM SDK. Also, these repositories also do five retries in case the flow fails for any reason.

4.2. Atala PRISM and Cardano Blockchain

4.2.1. Atala PRISM and the system

Atala PRISM is a self-sovereign identity platform and service suite for verifiable data and digital identity. Built on the Cardano blockchain, it offers core infrastructure for issuing DIDs and verifiable credentials, alongside tools and frameworks to help expand the ecosystem.

It utilizes Cardano as a verifiable data registry (VDR), functioning as a layer-2 blockchain solution.
The core concept of PRISM revolves around self-sovereign identity, empowering users to have control over their identity and personal information. Through the use of asymmetric cryptography, users securely share their data and choose with whom to share it.

4.2.1.1 Key Features:

- Decentralized identity solution built on the Cardano blockchain.
- Leveraging decentralized, self-sovereign identity, and verifiable credentials concepts.

- Enables individuals to own and manage their identity and credentials.
- Allows to securely share the verifiable credentials with the verifiers, facilitating various use cases across multiple sectors.

For more information about Atala PRISM, it is recommended to visit Atala PRISM

4.2.1.2 Functionality and Documentation:

- Atala PRISM utilizes functionally modular building blocks, reusable libraries with specific domain context bounds.
- PRISM Cloud Agent, PRISM Node, and other components provide detailed information and documentation.
- Feature-rich SDKs are available for building Apple SSI Applications (Swift SDK), Web SSI Applications (Typescript SDK), and JVM-based SSI Applications (Kotlin Multiplatform SDK).

Atala PRISM empowers individuals and businesses with a robust decentralized identity solution, ensuring data protection, security, and control. By leveraging the Cardano blockchain, it offers a reliable and interoperable infrastructure for managing digital credentials in a self-sovereign manner.

Atala PRISM can be used by an institution for two specific purposes: to generate DIDs and VCs for hierarchical institutions involved and also students enabling them to prove that they graduated, that they received a certain grade in an exam and to enable them to show a verifiable transcript of their school term.

4.2.1.3.1 DID Issuing and Processing

DIDs are generated for two types of use cases in the IOG system - for the institution/entity and for the user.

- Issuer/Institution DID Generation and Processing: Navigated by the First Admin of the institution (the First administrator that is created by the higher parent entity), DIDs get issued once per institution, and the rest

of the administrators are using that single Institution DID (shared in the backend) to create and sign transactions.

- Holder/Users DID Generation and Processing: In the case of DID generation for Holders (Students and Teachers) to be specific, the respective DID is generated and stored on their device's drive and the database and showing up under their profile.

4.2.1.3.2. Verifiable Credentials Processing

Generally, there are two types of verifiable credentials issued at any level:

- **Endorsement VCs:** is a type of credential, which is issued for lower level entities by a higher level endorsing institution. These credentials hierarchically give lower entities to issue transcript VCs culminating at the school. They follow the on ground endorsement hierarchy for a school to issue transcripts.
- **Transcript VCs** are issued for those with a "Holder DID" type (i.e: Students), and primarily consist of student's grade results/report cards stored as credentials.

DID issuing happens per DID/VC or in batches.

4.2.2. Cardano blockchain and the system:

Cardano is a proof-of-stake blockchain platform that was founded on peer-reviewed research and developed through evidence-based methods. It is an open-source and decentralized platform, with consensus achieved using proof-of-stake.

The main purpose of integrating the Cardano blockchain into the solution is to provide a robust framework for immutability and tamper-proof capabilities. When an issuer's DID is generated by the Atala PRISM service, it undergoes a hashing process and is then published on the blockchain. This allows the issuers (in this case, institutions managed by their administrators) to access and utilize the published DIDs.

At the end of each school year, when verifiable credentials are issued to students, these credentials are in JSON format and contain essential information such as grades, endorsements, issuers, and more. To ensure the integrity and security of these credentials, they are hashed and published to the Cardano blockchain.

When a verifier needs to authenticate a specific digital transcript or credential shared by a student or employee, they visit the verification portal. By providing the JSON-formatted credential or scanning the corresponding QR code, they instantly verify the authenticity of the provided record. The blockchain serves as an immutable ledger, enabling verifiers to confidently assess the legitimacy of the shared information.

4.2.2.1 Technical aspects of the Cardano Blockchain:

- **Peer-reviewed research:** Cardano distinguishes itself by being the first blockchain platform to be founded on peer-reviewed research. This ensures that the technology is rigorously tested and validated by experts in the field.
- **Proof-of-stake:** Unlike traditional proof-of-work blockchains, like Bitcoin, Cardano uses a proof-of-stake consensus mechanism. This means that instead of miners competing to solve complex mathematical puzzles, validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral.
- **Smart contracts:** Cardano is designed to run decentralized applications through smart contracts. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They enable the automation of transactions and the execution of complex business logic on the blockchain.

4.2.2.2 Functional aspects of the Cardano blockchain:

- **ADA cryptocurrency:** Cardano has its own native cryptocurrency called ADA. ADA is used for various purposes within the Cardano ecosystem, including staking, transaction fees, and as a medium of exchange.
- **Scalability and sustainability:** Cardano aims to be a flexible, sustainable, and scalable blockchain platform. It is designed to handle transactions in

a highly secure manner and to support the growth of decentralized applications and services.

- **Interoperability:** Cardano is conceived with interoperability in mind, allowing different blockchains and systems to communicate and interact with each other. This enables seamless integration with existing infrastructure and facilitates the development of cross-chain applications.
- **Ongoing development:** Cardano is continuously evolving and improving through regular updates and protocol upgrades. The development team is committed to ensuring the security, stability, and functionality of the platform.

  Overall, Cardano is a blockchain platform that combines rigorous research, proof-of-stake consensus, smart contracts, and scalability to provide a secure and efficient infrastructure for decentralized applications and services.

4.3. Architecture and technical considerations

This Digital Educational Credential system is an integrated ecosystem that leverages the Atala PRISM identity platform, empowering students, teachers, leaders, and staff members of the issuing instiution with complete control over their institutional and personal identities.

The system consists of both scalable back-end(s) and user-friendly front-end(s), ensuring a seamless user experience. The backend systems are designed using Domain-Driven Design (DDD) principles, enhancing the scalability and maintainability of the overall system. By incorporating best practices such as Kafka for real-time data processing, the back-end systems efficiently handle a large volume of events.

One of the key components of the system is the DID service, which acts as a bridge between the systems and the blockchain. It utilizes the Atala PRISM SDK, enabling secure interaction with the blockchain. The back-end systems leverage this service to send various events to the blockchain using topics, ensuring a secure and reliable connection.

The utilization of Atala PRISM SDK and the integration with the blockchain allows for the secure storage and verification of digital credentials. By adopting decentralized identity principles, the system ensures that individuals have full control over their identities and securely manage their credentials.

The Digital Educational Credential System integrates with Atala PRISM, providing a scalable backend architecture and user-friendly frontend interfaces. By incorporating DDD principles and utilizing the Atala PRISM SDK for blockchain interaction, the system enables secure and efficient management of digital credentials for the issuing instiution.

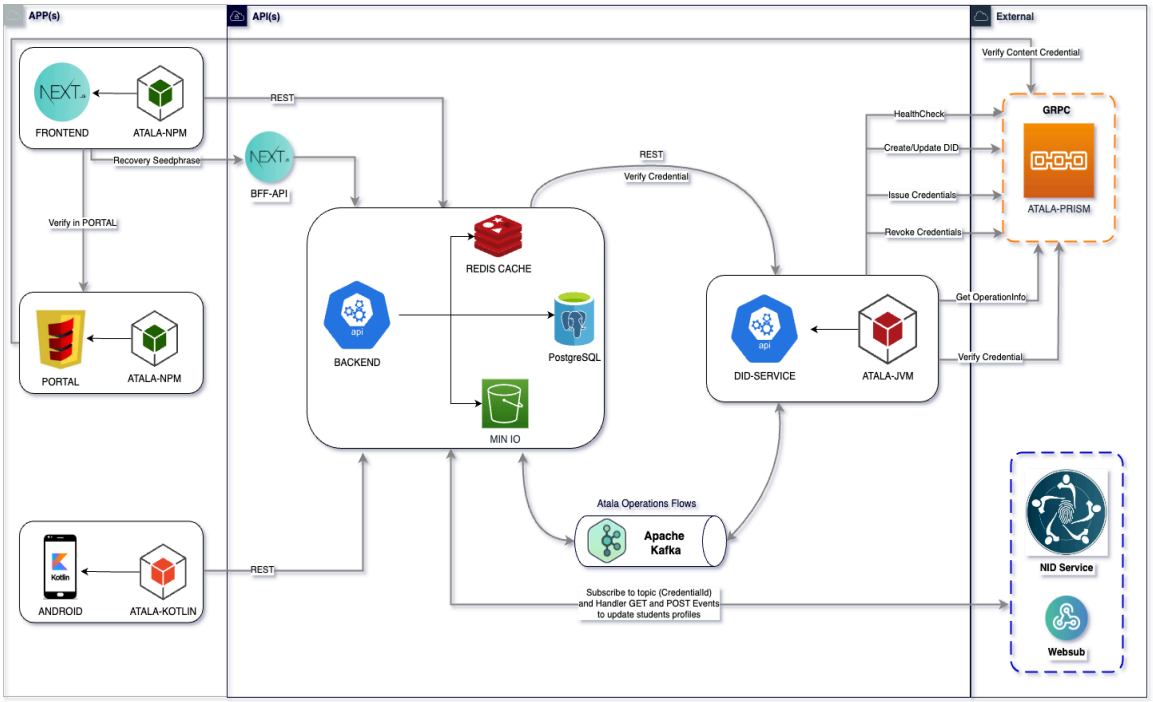

Image_08: Digital Credential API Integration

4.4. Data Security and Privacy Measures

4.4.1. General security consideration

The security of the system is of utmost importance, and as such, IOG has considered the security strategy described below.

Technology selection: Authentication for horizontal calls between microservices have been implemented using mutual Transport Layer Security (mTLS). This is

made possible through the utilization of Nomad and Vault, ensuring secure communication between the services. Notably, the usage of Vault replaces the need for a separate private key vault. Vault serves as a secure KeyValue store, accessed through the BFFs (Backend for Frontend), when an authenticated user requests it.

4.4.2. Data Security Considerations

Inflight data: All data transmitted between student/administrator/teacher devices, the frontend, and the backend is encrypted using TLS (Transport Layer Security). This ensures the security of the data during transit.
Security certificates are utilized, and it is recommended that the issuing instiution manages a free certificate service, such as Let's Encrypt, which provides automated and open certificates. This approach enhances the security of user passwords and other sensitive records.

- **Data at rest:** The current version of Postgres implemented does not support encryption, so data is stored unencrypted on the database servers, except for user passwords, which are properly encrypted. It is recommended that the issuing instiution performs encrypted backups of the data for added security.
- **Private keys:** The private keys of users (holders and issuers) are stored securely in a dedicated vault. These private keys are never transmitted to the backend in plain text. Instead, they are encrypted/decrypted by the client using the client's login password. The passwords adhere to minimum complexity rules. Storing the private keys in a vault provides a backup solution in case a device is lost or the user forgets their password. It also allows teachers and administrators to use different computers within the system, as they won't be limited to a single dedicated machine. For mobile applications, private keys can also be stored in the Android Keystore using the mentioned encryption scheme.
- **JWT (JSON Web Token):** In the case of mobile applications (native applications), JWTs are stored in the local storage. For web applications, JWTs are stored in cookies, ensuring secure token management.

Passwords are securely hashed and stored using the bcrypt+salt mechanism in the database, ensuring the confidentiality of passwords. To reinforce security, the

utilization of security certificates, https://letsencrypt.org has been deployed for enhanced protection.

By implementing these security measures, including encryption, secure storage, and recommended certificate services, the system aims to maintain the highest level of data security and protect user privacy.

4.5. Integration with National ID and other existing systems

The current solution can be successfully integrated with a national ID organisation (NID), enhancing the identity-centric aspect of the system. This integration enables the accurate identification of each student, teacher, and administrator within the system. Furthermore it ensures a unique step of registration, and the link with the unique Citizen National ID number. With the NID integration, external parties interacting with the institution system easily and effectively identify the users they are engaging with.

- **External integration capability:**

The current solution is designed to support seamless integration with external systems, establishing valuable partnerships. To enable this, a comprehensive API with a range of endpoints is provided. This API offers flexibility in specifying permissions for each integration. Some of the potential partners in this context include ministries for labour and transportation. By utilizing the partner API, these partners integrate with the institution system and securely access specific data as defined in the agreement and permission settings.

The API integration is using REST as a form of interaction with outside parties while the documentation is captured by SwaggerUI.

Through these integrations, the institution's system fosters collaboration, data sharing, and streamlined processes with external entities, ultimately enhancing the functionality and effectiveness of the education ecosystem.

The transition process for students entering higher education is considerably improved by integrating universities into the digital educational credential system. The technology automatically fills out university applications by combining electronic transcripts and exam results from schools, expediting the application process. Also, the usage of shared digital student IDs enables easy access to different institutions for students. The transfer and admissions

processes are further reduced by the use of standardized credentials, which makes it simpler for students to move across universities.

Universities also add to students' files by providing digital micro certificates for online courses, which serves as a full record of their schoolwork. The addition of online course credentials strengthens the student's academic profiles and shows their dedication to lifelong learning. There are several opportunities to expand the use of digital credentials in higher education. It supports an organized strategy for continuous education and aids in reducing unnecessary administrative task duplication. Students more effectively demonstrate their abilities and qualifications to hiring managers or pursue additional education possibilities with an integrated overview of educational achievements across several institutions.

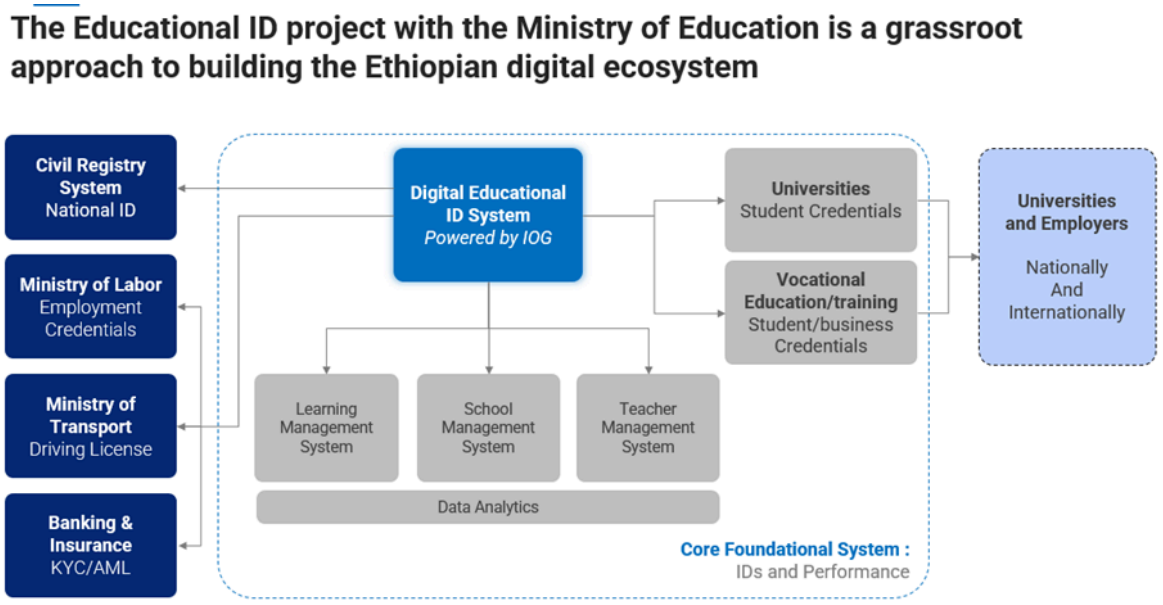

Image_9: Core Foundational System

4.6. Scalability and accessibility

The technology stack selection is part of the IOG application development standards framework, which enforces the deployment and use of the most stable and latest version of tools in projects. The software components in section 4.2.1 can be deployed and managed on-premises.

Several deployment approaches and tool stack can be used to ensure scalability across the entire system:

- **Orchestrator + service mesh:**

In the Ministry of Education implementation, due to the scale of the system, the large number of services running, and the deployment in the private cloud of the Ministry of Education, an orchestration and service mesh were needed to handle all of these efficiently. The technology used for these services needed to be well understood by the industry, supported, capable of handling a significant volume of data, open-source, and able to handle connection issues gracefully.

Technology selection: As an orchestrator and service mesh, Nomad and Consul were chosen. Other tools analyzed included Kubernetes, Istio, and Linkerd. The benefits of choosing Nomad included easy sharing of secrets between different services (with the help of Vault, which Istio did not provide out-of-the-box) and a simpler setup compared to Kubernetes+Istio. Nomad was widely used and had sufficient documentation/resources, making it a battle-tested tool.

- **Message broker:**

A reliable message broker was required to handle all incoming requests. The message broker needed to be able to scale gracefully and support the PubSub pattern.

Technology selection: Kafka and RabbitMQ were well-known projects chosen for their scalability and performance. The main reason for favoring Kafka was the durability of the messages. The message broker needed to handle outages and failures effectively. Additionally, Kafka's message durability allows for infinite retention of messages if necessary for data analytics, disaster recovery, or other needs, making it the best solution for an unstable internet connection.

- **Proxy (Load balancing and caching):**

  To handle the expected load, a service was needed to redirect calls to the individual process that could solve the query. This required a load-balancing proxy almost everywhere. Ideally, this service should be able to handle errors in the underlying services and connect directly to the message broker. Additionally, a caching mechanism was needed in the proxy to avoid reprocessing the same queries.

  Technology selection: Traefik was a tool that could handle the traffic needed. It was straightforward to use with Nomad compared to other alternatives like NGINX. It could manage certificates easily, had caching mechanisms, and could connect directly with Kafka. NGINX could not do this directly. Despite using NGINX for the static content server, Traefik was considered a better choice due to the listed reasons, even if it increased the tech stack.

- **Static content server:**

  A server was needed to provide static content to the users, including the web app and any type of legal text and/or images that needed to be downloaded by the mobile app. This service also received a lot of traffic, requiring redundancy and scaling.

  Technology selection: NGINX was the chosen tool for this purpose. It was performant, well understood by the industry and the company, and relatively easy to configure. Traefik was not able to fulfill this role at all.

The IOG system is designed to manage the increased demand during peak seasons to handle the issuance of millions of transcripts (VCs) using batching, message brokers, and in memory databases. Atala PRISM has also been tested to ensure its design can handle millions of DIDs and VCs issuance.

5. Ministry of Education

5.1 Case Study 1 : Secure Student Registration and National ID Integration with Atala PRISM

Background

As the Ministry of Education seeks to modernize student registration and integrate with the National ID system, the implementation of Atala PRISM has emerged as a groundbreaking solution. This case study highlights the seamless integration of student credentials, the incorporation of biometric data, and the transformation of identity verification processes.

Integration with National ID System

Upon enrollment, students' credentials are referenced onto the Cardano blockchain through a bulk or manual import of their personal information. The integration with the National ID system allows the inclusion of students' biometric data, enhancing data accuracy for the National Examination.

Objectives:

- **Decentralized identity management:** The primary goal was to establish a decentralized identity management system that guarantees security and privacy.

- **Personal data control:** Empower individuals to manage their personal data and disclose only essential information.
- **Trustworthy endorsement mechanism:** Offer institutions a secure and impervious mechanism for endorsing users.
- **Efficient identity verification:** Enhance identity verification procedures' efficiency and reduce associated costs.

Implementation Details:

User Onboarding:

- Admin Users create students' digital identities through registering on the IOG Digital Educational Credential System, and then link it to the SSI platform.
- DIDs and verifiable credentials are generated and linked to cryptographic key pairs.
- Users have the freedom to select which institutions to share their verified credentials with to obtain endorsements.

Institution endorsements:

- Participating institutions, including universities, employers, and government organizations, digitally sign user credentials using their private keys.

- These endorsements are certified and recorded on the blockchain, ensuring their immutability and traceability.

Credential verification:

- Organizations and relying parties can validate the legitimacy and integrity of a user's credentials by examining the digital signatures and endorsements stored on the blockchain.
- Manual verification processes become obsolete.

Advantages:

- **Enhanced security:** Blockchain's decentralized nature guarantees data integrity and security against unauthorized access and alterations.
- **Privacy and control:** Users retain full control over their personal data, sharing information only with trusted entities to mitigate identity theft and data breaches.
- **Efficient endorsement process:** Secure endorsement without intermediaries streamlines productivity and reduces expenses**.**
- **Immutable records:** Endorsements recorded on the blockchain offer a tamper-resistant, auditable source of truth for identity verification.
- **Interoperability:** The SSI platform seamlessly integrates with existing identity protocols and standards, enhancing compatibility with various software programs and services.

Conclusion

In the Ministry of Education implementation, the integration of Atala PRISM into the student registration process and its collaboration with the National ID system represented a significant leap toward a secure, efficient, and privacy-centric identity management ecosystem. By leveraging blockchain technology, this initiative enhanced data security, empowers individuals, and ensures reliable endorsement mechanisms. The resulting benefits span from data protection to streamlined processes, establishing a benchmark for identity management in the education sector.

5.2 Student User Experience: Solomon's journey

Background

Solomon is an ambitious and tech-savvy 12th-grade student. With the integration of Atala PRISM into the student registration process, Solomon's journey through education becomes more secure and transparent, paving the way for a digital future.

Step 1: Enrollment

- Solomon begins the enrollment process at his school. He learns that the school now uses Atala PRISM for student registration, which piqued his curiosity.

Step 2: Digital identity creation

- During enrollment, Solomon's digital identity is created by the school administrator on the system, using the Atala PRISM infrastructure and protocol. The system generates Solomon's verifiable credentials and connects it to his personal information.

Step 3: Credential generation and issuance

- At the end of each year, the school, validated via the school administrator, generates the transcript of Solomon having its grade results and other behavioral data, which will be converted to a verifiable credential. The hash of this credential will then get published to the Cardano Blockchain.

Step 4: Biometric data integration

- Solomon learns that his biometric data will also be linked into the system for enhanced security through his National ID unique number; however it will be safeguarded throughout the process due to the network's inherent benefits.

Step 5: National ID connection

- Solomon discovers that through his unique citizen National ID, his integration with the National ID system ensures the accuracy of his biometric data, which will play a role in the authentication by the Examination Agency.

Step 6: Selective sharing

- As Solomon explores the platform, he realizes he has control over which institutions to share his verified credentials with for endorsements. This empowers him to take back ownership of his personal data.

Step 7: Verification

- Universities and potential employers have the possibility to verify the authenticity of Solomon's identity and achievements.

Step 8: Efficient processes

- Solomon notices that verification of his credentials is faster and smoother, due to the blockchain's ability to eliminate the need for time-consuming manual verification.

Benefits for Solomon:

- Digital ownership: Solomon gains ownership of his digital identity and academic achievements, giving him a sense of control.
- Data security: Knowing his data is referenced on the blockchain assures Solomon that it's secure and tamper-proof.
- Efficiency: Faster verification processes mean Solomon can focus more on his studies and future aspirations.
- Transparency: Solomon values the transparent and trustworthy nature of endorsements stored on the blockchain.

Solomon's Perspective:

"Being a student in this digital age is exciting, especially with the integration of Atala PRISM into our education system. It's amazing to see my achievements securely referenced on the blockchain, and knowing that I have control over who sees my data makes me feel empowered. The fact that institutions can verify my credentials easily and efficiently is a game-changer. This technology is shaping a new and secure way for us to navigate education and beyond."

5.3 Case Study 2: Secure Institutions and User Endorsements through Atala PRISM Integration

Background

In an era where data security and trust are paramount, institutions and organizations in various sectors are seeking advanced solutions to secure endorsements and manage user identities. This case study presents the implementation of Atala PRISM, addressing

the security needs of institutions and individuals while ensuring endorsement processes are transparent and tamper-proof.

Objectives:

Decentralized identity management

The primary objective is to establish an uncrackable identity management system using a decentralized approach.

Personal data ownership

Empower individuals to own and control their personal data, safeguarding their digital identities.

Safe user endorsements

Provide institutions with a secure and transparent system for endorsing users, enhancing the credibility of the endorsement process.

Enhanced endorsement effectiveness

Boost the validity and effectiveness of endorsements, reducing the risk of fraud and misrepresentation.

Implementation details

Atala PRISM integration:

- Institutions integrate the Atala PRISM platform into their endorsement procedures.
- The Digital Educational Credential system platform is customized to align with each institution's unique needs and procedures.

User registration:

- Users establish their digital identities on Atala PRISM by creating a cryptographic key pair and a unique decentralized identifier (DID).
- Users have complete control over their identifying information, ensuring ownership and privacy.

Credential issuance:

- Organizations issue verified credentials, such as diplomas, to users.
- These credentials are cryptographically signed by the issuing institution, ensuring validity and integrity.

Decentralized endorsements:

- Institutions endorse users by digitally signing their verified credentials through the Atala PRISM platform.
- These endorsements are securely referenced on the Cardano blockchain, providing transparency, immutability, and traceability.

Verification process:

- Institutions and authorized parties access the system verification portal of the Cardano blockchain to verify the legitimacy and authenticity of endorsements.
- The blockchain's decentralized architecture ensures endorsements cannot be altered or tampered with.

Benefits and outcomes:

- **Unbreakable security**: Atala PRISM integration ensures a highly secure and decentralized identity management system, reducing the risk of identity-related fraud.
- **Personal data control**: Individuals have complete ownership and control over their personal data, promoting digital autonomy.
- **Institutional trust**: Institutions benefit from a secure endorsement process, fostering trust and credibility among stakeholders.
- **Transparent endorsements**: The transparent and traceable nature of endorsements on the blockchain enhances overall endorsement process integrity.
- **Fraud prevention**: Decentralized endorsements minimize the possibility of fraudulent or misrepresented endorsements.

Conclusion

The integration of Atala PRISM into institutions' endorsement procedures showcases an innovative approach to achieving secure identity management and transparent endorsement processes. By leveraging blockchain technology and decentralized identities, this initiative safeguards personal data, enhances trust, and sets new standards for the credibility of endorsements. As a result, organizations and individuals alike can benefit from heightened security and reliability within the endorsement ecosystem.

5.4 School administrators' experience: Ahmed's journey

Background

Ahmed is a diligent and forward-thinking school administrator responsible for managing various aspects of his institution. With the integration of Atala PRISM into the endorsement procedures, Ahmed's role becomes more streamlined and secure, enhancing the credibility of user endorsements and data management.

Step 1: Introduction to Atala PRISM

- Ahmed learns about the Atala PRISM platform and its potential to revolutionize endorsement processes and data management in educational institutions.

Step 2: Recognizing the benefits

- Ahmed recognizes that Atala PRISM offers a decentralized and secure solution for endorsing users and managing their identities, addressing some of the common challenges in traditional endorsement methods.

Step 3: Integration and implementation

- Ahmed is able to integrate Atala PRISM into the school's endorsement procedures. He coordinates with his team to ensure a seamless implementation process.

Step 4: Enhancing data security

- Ahmed observes that the cryptographic key pair and decentralized identifier (DID) approach offers a higher level of data security for both the institution and the endorsed users.

Step 5: Streamlined endorsements

- As institutions endorse users by digitally signing their verified credentials, Ahmed notices a significant reduction in the administrative effort required for endorsements.

Step 6: Improved transparency

- Ahmed appreciates the transparency provided by the blockchain, as all endorsements are securely documented and tamper-proof, enhancing the credibility of endorsements.

Step 7: Effortless verification

- Ahmed's team finds that verifying endorsements has become much more efficient. They can access the Cardano blockchain through the system verification portal to validate endorsements swiftly and reliably.

Step 8: Testimonial to Stakeholders

- Ahmed shares his positive experience with the school's stakeholders, explaining how the integration of Atala PRISM has revolutionized endorsement procedures and data security.

Benefits for Ahmed:

- **Efficiency**: Ahmed witnesses a reduction in administrative efforts related to endorsement processes.
- **Enhanced Data Security**: The decentralized approach offers a more secure way to manage user data and endorsements.
- **Credibility**: The blockchain-based endorsements enhance the credibility of the institution's endorsement procedures.
- **Transparency**: The transparent and tamper-proof nature of endorsements enhances trust among stakeholders.
- **Streamlined Verification**: Verification becomes easier and more efficient through the blockchain.

Ahmed's Testimonial

"The integration of Atala PRISM has brought a new level of efficiency and security to our endorsement procedures. Our institution now has a decentralized and tamper-proof way of endorsing users, which has not only streamlined our processes but also enhanced the credibility of our endorsements. The transparency and security provided by the blockchain have exceeded our expectations. I am confident that this innovative solution will set new standards in endorsement processes within educational institutions." Ahmed school admin

5.5 Case Study 3: Ensuring Data Immutability through Atala PRISM Integration

Background

With a firm commitment to safeguarding student data and ensuring its unalterable integrity, the Ministry of Education has embarked on a pioneering initiative. The goal was to create a decentralized architecture that ensures data immutability within the education system. This case study delves into the details of implementation and the transformative impact on data security and transparency.

Objectives:

- **Decentralized data immutability**: The primary objective is to establish a decentralized framework that guarantees the permanence and immutability of student data records, eliminating the possibility of unauthorized changes or tampering.
- **Empowerment and ownership**: By allowing students to have ownership and control over their personal data, the initiative aims to empower them while enhancing data security.
- **Enhanced data integrity**: The initiative seeks to enhance the overall integrity of school management systems by ensuring the veracity of student records.

Implementation details:

- **Integration with Atala PRISM:**
    - The school management system seamlessly integrates with the Atala PRISM platform, leveraging its decentralized identity and verified credential capabilities.
- **Student Registration:**
    - School administrators initiate the students registration process through the Atala PRISM platform, constructing their unique digital identities.
    - Verifiable credentials are generated, connecting it to students' personal information, putting students in charge of their data.
- **Data storage on the blockchain:**
    - While verifiable credentials, such as diplomas and certificates, are stored on the Cardano blockchain, personal data records like academic accomplishments, attendance, and disciplinary history are stored off-chain.
    - The blockchain ensures data immutability and transparency, guarding against unauthorized modifications**.**
- **Verifiable credentials:**

    - Educational institutions issue verifiable credentials to students, including diplomas and certificates.
    - These credentials are authenticated and secured through cryptographic signatures and blockchain storage.
- **Data access and consent:**
    - Students are granted the authority to selectively share their personal information with authorized parties such as employers and educational institutions.
    - Consent for data access is managed through the Atala PRISM platform, enhancing privacy and control.
- **Data verification:**
    - Educational institutions and any entities can access the Cardano blockchain to validate the authenticity of individual data entries.
    - Manual verification procedures are rendered obsolete, ensuring data reliability and accuracy.
- **Benefits and outcomes:**
    - **Immutable data records**: The integration with Atala PRISM guarantees the immutability and permanence of student data, enhancing the integrity of records.
    - **Student empowerment**: Students gain ownership of their personal data, exerting control and enjoying enhanced digital autonomy.
    - **Enhanced transparency**: The transparency enabled by the blockchain fosters trust among stakeholders in the education system.
    - **Data security**: The initiative fortifies data security, ensuring that records remain unchanged and tamper-proof.
    - **Streamlined verification**: The decentralized data verification process eliminates the need for resource-intensive manual verification, saving time and effort.

Conclusion

The Ministry of Education's collaboration with IOG has resulted in a trailblazing solution that ensures the immutability of student data. By integrating blockchain technology and decentralized identity, the Ministry set a new standard for data security, ownership, and transparency within the education system. This initiative not only safeguards student records but also empowers them while enhancing the overall credibility of educational achievements.

5.6 Teacher user experience: Betty’s journey

Background

Betty is a dedicated and passionate 10th-grade teacher at a school. She is committed to providing quality education to her students and is excited about the Ministry of Education's new initiative to ensure data immutability within the education system. This initiative, implemented through the integration of Atala PRISM, brings a transformative change to how data is managed and secured.

Step 1: Introduction to the initiative

- Betty learns about the Ministry's new initiative to ensure the immutability of student data within the education system.

Step 2: Understanding the benefits

- Betty discovers that this initiative will enhance the security and permanence of student records, ultimately benefiting both teachers and students.

Step 3: Integration with Atala PRISM

- As the initiative rolls out, Betty’s school integrates the school management system with the Atala PRISM platform, known for its blockchain-based data security features.

Step 4: Accessing the system

- Betty logs into the system using her credentials, noting the user-friendly interface designed to simplify data management tasks.

Step 5: Recording student data

- Betty enters attendance records, exam scores, and other student-related information, confident that the system will ensure the immutability of these records**.**

Step 6: Embracing data integrity

- As Betty records data, she appreciates the peace of mind that comes from knowing that the blockchain technology used in the system guarantees the integrity and permanence of the records**.**

Step 7: Efficient verification

- Betty realizes that the data she records is tamper-proof and can be verified efficiently through the blockchain, saving time and ensuring data accuracy.

Step 8: Student engagement

- Betty discusses this initiative with her students, educating them about the importance of data security and the benefits of having verifiable records.

Step 9: Embracing transparency

- Betty enjoys the transparency brought by the system, knowing that she, her students, and parents can trust the integrity of the information stored.

Benefits for Betty:

- **Enhanced data security:** Betty appreciates the increased data security and immutability ensured by the Atala PRISM integration.
- **Simplified data management:** The user-friendly interface makes recording and managing student data more efficient**.**
- **Trust in records:** Betty is confident that the data she records will remain accurate and unaltered, fostering trust in the education system**.**
- **Streamlined verification:** The blockchain's verification process simplifies and expedites record verification, saving her time.
- **Educational opportunities:** Betty uses the initiative to educate her students about the importance of data security and transparency**.**

Betty's user experience illustrates how the Ministry's initiative, powered by Atala PRISM, transforms data management for teachers, ensuring data immutability, security, and transparency.

Betty’s testimonial:

"The Ministry's initiative to ensure data immutability through Atala PRISM has truly transformed how we manage student records. As a teacher, knowing that the data I enter maintains its integrity is invaluable. The integration of blockchain technology simplifies verification processes, saving time and increasing the reliability of records. What's even more heartening is that I can educate my students about data security and the power of transparent information. This initiative is a game-changer in enhancing trust and efficiency within the education system."

5.7 Case Study 4: Achievements verification through a verification portal

Background

In a dynamic move towards modernizing the education sector, the Ministry of Education integrated a decentralized verification portal into its Digital Education System. This strategic initiative was designed to establish a secure and robust framework for verifying individuals' achievements. By partnering with IOG to use its Atala PRISM platform, the Ministry aims to leverage decentralized identity and verifiable credential features, thereby revolutionizing the authenticity and efficiency of achievement verification.

Objectives

The primary objective is to create a transparent and secure framework for confirming individuals' accomplishments within the Digital Education System. The portal aims to streamline the verification process while ensuring data security and accuracy.

Enhanced legitimacy

By harnessing the power of decentralized identities and verifiable credentials, the Ministry seeks to elevate the legitimacy and integrity of achievements within the education system. This initiative aims to instill trust and confidence in verified accomplishments.

User empowerment

The Ministry's goal is to grant individuals ownership and control over their achievement data. By enabling users to manage and selectively share their verifiable credentials, the system empowers users to take charge of their educational achievements.

Efficiency and cost savings

Through the integration of a decentralized verification portal, the Ministry aims to enhance productivity and significantly reduce expenses associated with traditional manual verification processes. Automation and secure validation contribute to resource optimization.

Implementation details

- **Integration with Atala PRISM:**

Seamlessly integrated with the Digital Education System, the verification portal taps into Atala PRISM's decentralized identity and verifiable credential capabilities.

- **Achievement issuance**

Educational institutions within the Ministry issue verifiable credentials upon individuals achieving educational milestones. These credentials are securely signed by the issuing institutions and anchored on the immutable Cardano blockchain.

- **The verification process:**

Individuals conveniently submit their verifiable credentials through the Ministry's Digital Education System for authentication. Leveraging the Cardano blockchain's robust security, the portal ensures the accuracy and reliability of the verification process.

- **Privacy and control**

Users maintain full control over their achievement data, utilizing the system web app or mobile app to selectively share verifiable credentials as needed. This user-centric approach reinforces data ownership and safeguards privacy while allowing data sharing.

- **Decentralized validation:**

The verification portal harnesses Atala PRISM's decentralized identity infrastructure for seamless verification of credentials. This decentralized approach not only enhances accuracy but also reduces the risk of fraudulent claims.

- **Increased efficiency and lower costs:**

Automating the verification process enhances efficiency within the Digital Education System, reducing administrative burdens. Organizations and institutions benefit from quicker, more cost-effective verification.

Benefits and Outcomes:

- **Enhanced credibility**: Atala PRISM's integration bolsters credibility, fostering trust in achievements issued and verified within the Digital Education System.

- **Empowered individuals**: Users gain authority over their achievement data and sharing thereof, thereby reinforcing data ownership and privacy.
- **Streamlined verification**: The Digital Education System's decentralized validation expedites the verification process, saving time and resources.
- **Data security**: Utilizing verifiable credentials and blockchain technology ensures secure, immutable achievement data.
- **Fraud mitigation**: Decentralized validation minimizes the potential for fraudulent claims, safeguarding the integrity of accomplishments.
- **Innovation leadership**: The Digital Educational Credential System, using Atala PRISM's platform, aligns the Ministry of Education with global trends in decentralized identity, establishing a pioneering position.

Conclusion

The Ministry of Education's integration of a decentralized verification portal into its Digital Education System, through the integration of Atala PRISM, signifies a paradigm shift in education credential verification. By leveraging cutting-edge technology, this initiative not only streamlines processes and fosters trust but also empowers individuals with ownership and control over their achievements. The Ministry of Education is at the forefront of revolutionizing education verification, setting new standards for efficiency, authenticity, and security within the Digital Education System.

5.8 Student Experience of the verification portal : Kidist journey background

Kidist is a diligent and ambitious 12th-grade student. She is excited about her future and is actively exploring opportunities for higher education. With the Ministry of Education's integration of a decentralized verification portal within the Digital Education System, Kidist's journey towards achieving her educational goals becomes even more streamlined and empowering.

Step 1 : Enrollment and account creation

- Kidist receives information from her school about the new decentralized verification portal as part of the Digital Education System.
- Kidist receives her credentials from the school admin who has processed her enrollment in the system
- Intrigued, she visits the portal's website

Step 2 : Uploading verified credentials

- Kidist logs into her portal account and is thrilled to find a dedicated section for uploading her verifiable academic credentials.
- She carefully uploads her verified high school diploma, certificates, and other accomplishments.

Step 3 : Tailoring privacy settings

- Kidist takes a moment to explore the privacy statement. She decides who can access her credentials, ensuring her control over her data.

Step 4 : Applying for universities

- As Kidist prepares to apply to various universities, she's delighted to see that some of them recognize and support the decentralized verification portal.
- She includes a link to her portal in her university applications, knowing her credentials will be securely verified.

Step 5 : Swift and reliable verification

- Kidist starts receiving notifications from universities indicating that her credentials have been successfully verified.
- She's impressed by the speed and accuracy of the process, which saves her time and eliminates concerns about the legitimacy of her achievements.

Step 6 : Scholarship opportunities

- Excitedly, Kidist discovers that her verified achievements have made her eligible for specific scholarships.
- She applies confidently, knowing her credentials are already authenticated through the portal.

Step 7 : Acceptance and beyond

- Kidist receives acceptance letters from her preferred universities.
- She confidently accepts an offer, excited to start the next chapter of her educational journey.

Step 8 : Securely managing her achievements

- Kidist continues to log into the system, appreciating the ease of access to her verifiable credentials.
- She selectively shares her achievements with future employers and mentors, maintaining control over her data.

Benefits for Kidist

- **Simplicity and convenience:** The portal's user-friendly interface ensures Kidist's smooth enrollment and credential uploading process.
- **Control and ownership:** Kidist's ability to manage her privacy and control data access empowers her.
- **Time savings:** Swift verification of her achievements saves Kidist time during the university application process**.**
- **Confidence:** The portal's validation boosts Kidist's confidence in her applications and scholarship opportunities.
- **Streamlined journey:** Kidist experiences a streamlined transition from high school to higher education, setting a positive precedent for her future endeavors.

Kidist's user experience exemplifies the transformation brought about by the Ministry of Education's decentralized verification portal within the Digital Education System, providing students like her with efficient, secure, and empowering educational pathways.

Kidist's Testimonial:

"The Ministry of Education's decentralized verification portal has completely transformed how I approach higher education. The convenience of uploading and verifying my achievements through the Digital Education System saved me so much time during application season. What's truly empowering is that I have control over who accesses my data, giving me a sense of ownership. Thanks to this portal, I confidently applied for scholarships, and the verifiable credentials opened doors I never thought possible. The future is brighter with this innovative approach, and I'm grateful for the Ministry's dedication to streamlining our educational journeys." Kidist, 12th-grade student.

6. Other considerations

Input Output Global has designed the Digital Educational Credential System to provide the flexibility needed for issuing institutions to comply with local legal requirements. As far as specific regional or local considerations could be concerned, it is the responsibility of the clients and users to make sure proper institutions and human processes are being put in place in accordance with the solution usage. Below are listed a few considerations on this matter.

6.1. Compliance with data protection and privacy laws

In most jurisdictions, the issuing institution will be required to comply with rules and regulations that protect the privacy of an individual's data. This may involve obtaining explicit consent from students or their guardians before collecting and processing their data. Local regulations may require the appointment of a Data Protection Officer to oversee compliance and ensure that data is stored securely, and access is restricted to authorized personnel only.

6.2. Ethical implications of digital educational credential systems

A country's cultural and socioeconomic landscape must be carefully considered when implementing a digital educational credential system to identify potential biases in algorithms and ensure that digital credentials do not exacerbate existing inequalities. By providing equitable access to digital resources and accommodating those without digital literacy, the client can uphold ethical standards.

6.3. Ensuring transparency and consent

Local rules and regulations may require an issuing institution to develop a comprehensive privacy policy that outlines the purpose, scope, and methods of data collection and usage. This policy should be communicated clearly to students, parents, and guardians. Consent mechanisms should be user-friendly and easily accessible. The client is also advised to establish processes for individuals to withdraw consent or request data deletion.

6.4. Empowering data owners

As part of its ethical responsibility, it is advisable that issuing institutions provide students with a user-friendly portal to access their data. This means that in case of inaccurate information, students have the possibility to request a change. A verification portal should allow students to grant access to their digital credentials and decide who can verify them. By providing students the possibility to access, and request change of their data in case of issue, the client respects their autonomy and privacy.

6.5. Ethics in credential verification

Issuing institutions should ensure that the verification process is transparent and accountable. In cases of disputes or inaccuracies, a clear process for challenging verification results should be established. This approach guarantees that the system's integrity is maintained and that students' achievements are accurately represented.

6.6. Cultural sensitivity and respect

Cultural diversity is a significant factor in data collection and usage. Issuing institutions are advised to customize their communications to resonate with various cultures and languages. Cultural norms and sensitivities should be respected throughout the system's design, ensuring that all students feel valued and included.

6.7. Capacity building and education

Issuing institutions should prioritize educating stakeholders, including teachers, students, parents, and administrators, about the ethical use of digital credentials. Workshops, seminars, and informational campaigns can foster a deeper understanding of data privacy, consent, and the responsible use of technology.

The IOG Digital Educational Credential System has the potential to revolutionize education while upholding legal and ethical standards. By embracing data protection laws, addressing ethical considerations, ensuring transparency and consent, and respecting cultural diversity, the Issuing institution can set a progressive example. Through this holistic approach, the issuing institution not only enhances the educational experience but also establishes itself as an ethical leader in the integration of technology and education.

7. Outlook and innovation

The field of digital educational credential systems has seen significant advancements in recent years, and there are several potential future developments that could further enhance the effectiveness and efficiency of such systems. Here are a few potential advancements:

7.1 Educational institution management

7.1.1 Open standards and interoperability

To ensure the seamless exchange and verification of digital credentials across different platforms and systems, the development and adoption of open standards are crucial. Open standards facilitate interoperability and allow for the easy integration of credentialing systems with other educational technologies. Advancements in this area may involve the establishment of common data formats, protocols, and APIs (Application Programming Interfaces) that enable the secure and standardized transfer of credentials between various stakeholders.

7.1.2 Data analytics and learning analytics

Integration with data analytics and learning analytics technologies provide valuable insights into the effectiveness of Educational programs and the impact of credentials. By analyzing data from digital credentials, institutions and policymakers gain a better understanding of learner outcomes, identify areas for improvement, and make data-driven decisions to enhance the quality of education and training.

7.2 Authentication and fraud management

7.2.1 Microcredentials and digital badges

Microcredentials and digital badges are gaining popularity as alternative forms of Educational credentials. These credentials offer a more granular and modular approach to learning, allowing individuals to acquire specific skills or knowledge

in a particular domain. Future advancements may involve the development of standardized frameworks for microcredentials and digital badges, making them more widely recognized and accepted by employers and Educational institutions.

7.2.2 Enhanced security and privacy measures

As digital credential systems evolve, it is crucial to ensure robust security and privacy measures. Advancements in encryption techniques, secure authentication protocols, and data privacy frameworks help protect sensitive information and prevent unauthorized access or data breaches. Additionally, advancements in decentralized identity systems, such as self-sovereign identity, provide individuals with greater control over their personal data and privacy.

7.2.3 Biometric authentication

Biometric authentication technologies, such as fingerprint or facial recognition, are integrated into digital educational credential systems to enhance security and prevent identity fraud. Learners securely access and share their credentials using biometric authentication methods, ensuring the integrity and authenticity of the credentials.

These integrations enhance the functionality, security, and accessibility of digital educational credential systems, ultimately benefiting learners, educational institutions, and employers. However, it is important to consider privacy concerns and ethical implications when integrating emerging technologies with digital educational credential systems, ensuring that data protection and user rights are safeguarded.

7.3 Collaborative efforts and knowledge-sharing among institutions

Collaborative efforts and knowledge-sharing among institutions are crucial for the successful implementation and adoption of a blockchain-based credential management system. Here are some key aspects to consider:

7.3.1 Standards development

Institutions should collaborate to develop common standards and protocols for blockchain-based credential management. This includes defining data formats, verification processes, and interoperability standards. By establishing industry-wide standards, institutions ensure seamless integration and exchange of credentials across different systems and platforms.

7.3.2 Consortiums and partnerships

Institutions form consortiums or partnerships to pool resources, expertise, and infrastructure for implementing blockchain-based credential management systems. Collaborative efforts help in sharing knowledge, technology, and best practices, thereby reducing duplication of efforts and accelerating the adoption of the system.

7.3.3 Pilots and proof-of-concept projects

Institutions collaborate on pilots and proof-of-concept projects to test and evaluate blockchain-based credential management systems. These projects allow institutions to identify technical challenges, explore potential use cases, and gather feedback from stakeholders. Collaborative pilots also provide an opportunity to refine the system and address any scalability or interoperability issues.

7.3.4 Research and development

Institutions collaborate on research and development initiatives to advance the understanding and application of blockchain technology in credential management. By sharing research findings, exploring innovative approaches, and conducting joint studies, institutions collectively contribute to the development of more robust and efficient systems.

7.3.5 Knowledge-sharing platforms and events

Institutions establish knowledge-sharing platforms, such as online forums, communities of practice, or conferences, to facilitate the exchange of ideas, experiences, and insights related to blockchain-based credential management. These platforms provide a space for institutions to share challenges, successes, and lessons learned, fostering a collaborative environment for continuous improvement and innovation.

7.3.6 Policy and regulatory advocacy

Institutions collaborate to advocate for supportive policies and regulations that facilitate the adoption of blockchain-based credential management systems. By working together, institutions engage with policymakers, industry bodies, and

regulatory authorities to address legal and governance issues, ensure data privacy and security, and create an enabling environment for the implementation of these systems.

7.3.7 Capacity building and training

Collaborative efforts also extend to capacity building and training initiatives. Institutions join forces to develop training programs, workshops, and resources to educate stakeholders about blockchain technology and its application in credential management. By building a skilled workforce and promoting awareness, institutions drive the adoption of these systems more effectively.

Overall, collaborative efforts and knowledge-sharing among institutions play a vital role in advancing the implementation and effectiveness of blockchain-based credential management systems. By working together, institutions leverage collective expertise and resources to overcome challenges, ensure interoperability, and create a more seamless and trusted ecosystem for managing educational credentials.

7.4 Leveraging higher education with digital educational credential system

Leveraging higher education with a blockchain-based digital educational credential system brings about several benefits and opportunities. Here's how higher education is enhanced through the implementation of such a system:

7.4.1 Enhanced security and trust

Blockchain technology provides a secure and tamper-proof infrastructure for storing and managing educational credentials. By leveraging blockchain, higher education institutions ensure the integrity and authenticity of credentials, mitigating the risk of fraud and misrepresentation. This enhanced security and trust benefits students, employers, and educational institutions alike.

7.4.2 Streamlined credential verification

Verifying the authenticity of educational credentials is a time-consuming and resource-intensive process. With a blockchain-based credential system, higher education institutions streamline the verification process. The decentralized nature of blockchain allows for instant and secure verification, eliminating the need for manual checks and reducing administrative burdens.

7.4.3 Improved credential portability

Digital credentials registered on a blockchain are easily accessed and shared by students. This improves credential portability, enabling students to carry their verified achievements across different institutions, platforms, and even countries. It simplifies the transfer of credits, facilitates the recognition of prior learning, and supports lifelong learning initiatives.

7.4.4 Increased transparency and accountability

Blockchain provides a transparent and auditable record of credential issuance and verification. This transparency enhances accountability and ensures that the credentialing process is fair and unbiased. Students, employers, and educational institutions have confidence in the validity and accuracy of the credentials, promoting trust and integrity in the higher education ecosystem.

7.4.5 Facilitated credential innovation

Blockchain-based credential systems support the development and recognition of new types of credentials. For instance, microcredentials, digital badges, and competency-based credentials are seamlessly integrated and verified on the blockchain. This flexibility allows higher education institutions to adapt to evolving skill demands and provide learners with more diverse and targeted credentialing options.

7.4.6 Data-driven insights

The data stored on a blockchain is harnessed to gain valuable insights into student learning pathways, skill trends, and labor market demands. Higher education institutions leverage this data to make informed decisions about curriculum design, program development, and strategic planning. It enables evidence-based improvements in educational offerings and promotes alignment with industry needs.

7.4.7 Lifelong learning and continuing education

A blockchain-based credential system supports lifelong learning and continuing education initiatives. Students accumulate and showcase a comprehensive record of their learning achievements throughout their careers. This promotes continuous skill development, facilitates career advancement, and encourages a culture of lifelong learning.

7.4.8 Collaboration and partnerships

Blockchain-based credential systems facilitate collaboration and partnerships among higher education institutions. They work together to establish common standards, share best practices, and even create joint programs that recognize and accept each other's credentials. This collaboration expands opportunities for learners, encourages knowledge exchange, and fosters a more interconnected higher education landscape.

Implementing a blockchain-based digital educational credential system in higher education revolutionizes the way credentials are issued, shared, and verified. It promotes efficiency, transparency, and trust, ultimately benefiting students, employers, and educational institutions by creating a more robust and learner-centric credentialing ecosystem.

8. Cost-benefit analysis for educational institutions

In the pursuit of advancing educational capabilities, the implementation of an ducational Digital ID System demands a meticulous cost-benefit analysis. Such an evaluation is crucial to understanding the financial and operational implications of adopting this technology-driven solution. This section delves deeper into the various components of this analysis, emphasizing the multifaceted advantages that the system brings to Educational institutions.

8.1 Assessing the initial implementation costs

The initial implementation costs of an Educational Digital ID System encompass a range of factors. These include:

- **Technology acquisition:** This includes the procurement of software and hardware components required for the system's deployment. Costs may vary depending on the chosen technology stack, scalability requirements, and potential customization.
- **Software development and integration:** If the system requires bespoke software development or integration with existing systems (such as student databases or learning management platforms), associated costs should be considered.
- **Training and onboarding:** Budgeting for training sessions to familiarize staff and students with the new system ensures its successful adoption.

8.2 Analyzing long-term cost savings and efficiency gains:

The implementation of an Educational Digital ID System yields substantial long-term cost savings and efficiency gains:

- **Automation of administrative tasks**:
  Manual processes like attendance tracking, resource allocation, and identity verification is automated, saving valuable time and reducing labor costs.

  Example: The fact that information and results are compiled immediately by the system, and aggregated at every level, without risk of any fraud or mistake.

- **Reduction in paper-based processes**:
  The move away from paper-based identification methods translates into lower material and printing costs, as well as decreased administrative overhead.

  This means concretely

  - no more need to print various day to day and end of term / end of education year documents, including certificates
  - no more need of manual reporting, of manual consolidation of paper documents from school up to Ministry
  - no more need of transport of physical documents, which includes physical risk, manual fraudulent change of results
  - no more need to lose all archived documents and results due to building fire, water flooding, or even country conflict
  - no more need to allocate team members to collect, compile, control accuracy of physical reports

- **Minimized errors and fraud**: The system's robust identity verification mechanisms reduce errors and fraud, preventing potential financial losses associated with unauthorized access or security breaches.
- **Optimized resource utilization:** Efficient allocation of resources based on data-driven insights leads to reduced waste and better resource utilization.

While these initial costs appear substantial, it's essential to view them in the context of the broader institutional strategy. The potential for streamlined operations, improved security, and enhanced user experiences yield significant long-term benefits

8.4 Estimating return on investment (ROI) for educational institutions:

Calculating ROI involves a comprehensive assessment of both financial and non-financial benefits:

- **Financial benefits:** These include quantifiable cost savings from reduced administrative tasks, minimized errors, and optimized resource allocation. Additionally, potential revenue enhancement through increased operational efficiency and student satisfaction contributes to the financial benefits.
- **Non-financial benefits:** Improved security, enhanced student and staff experiences, and the institution's ability to adapt to modern technology trends are qualitative benefits that contribute to ROI. In addition, the institution does increase its national and international credibility, as all the results and credentials are authentified, and tamper proof

The formula to calculate ROI is:

$$\textit{ROI} = \text{Net return} \,/\, \textit{Cost of Investment} \times 100\%$$

A higher ROI indicates that the long-term benefits outweigh the initial costs, making the adoption of the Educational Digital ID System a prudent investment.

A thorough cost-benefit analysis for the implementation of an Educational Digital ID System reveals a compelling case for its adoption. While the initial investment may seem significant, the long-term cost savings, efficiency gains, and non-financial benefits contribute to a favorable ROI. Educational institutions stand to not only optimize their operations but also enhance their competitive edge in an evolving educational landscape. The meticulous evaluation of costs and benefits equips decision-makers with a data-driven foundation for embracing technology's transformative potential and steering their institutions toward a more efficient, secure, and technologically empowered future.

9. Economic impact on students and educational institutions staff

As eduction teams around the world strive to modernize their educational landscape, embracing advanced technologies has become crucial to enhance efficiency, accessibility, and inclusivity. The IOG system is a cutting-edge solution that leverages digital technology to streamline administrative processes, minimize costs, and foster inclusivity. This section of the white paper explores the various economic advantages of implementing such a system and emphasizes its transformative potential in addressing socioeconomic disparities in educational access.

9.1 Minimizing financial burdens on students for ID-related expenses

The implementation of the Educational DID system offers significant economic benefits for students and educational staff.

9.2 Improving productivity and time management for educational staff.

Traditionally, identification processes involve considerable costs for students, including fees for ID cards, documents, and verification. The introduction of an Educational ID System significantly reduces these financial barriers. By providing students with digital credentials, educational institutions ensure education remains affordable and accessible to all, regardless of their financial backgrounds.

9.3 Full digital (paperless) and secure solution, with limited logistical and staff costs

The transition to a full digital and paperless Educational ID system brings numerous benefits to educational institutions.

9.3.1 Logistical and staff cost reduction

The shift from physical documents to digital credentials significantly reduces logistical overhead, including printing, distribution, and storage costs. Moreover, the system's streamlined operations require fewer staff resources, leading to additional cost savings for educational institutions.

9.3.2 Enhanced security and fraud prevention

Digital ID systems offer robust security features, such as encryption and blockchain technology, ensuring that student data remains secure and tamper-proof. This enhanced security prevents identity fraud and unauthorized access to sensitive information, safeguarding the reputation of educational institutions.

9.3.3 Sustainability and environmental impact

The transition to a paperless system not only reduces operational costs but also has a positive environmental impact by saving paper and reducing waste. Educational institutions contribute to sustainability goals by adopting eco-friendly practices through digital IDs.

9.4 Addressing socioeconomic inequality in educational access

An advanced Educational ID system plays a crucial role in addressing socioeconomic disparities in educational access.

10 External economic benefits

Several countries face challenges related to the digital divide, particularly for students from economically disadvantaged backgrounds. The IOG Educational ID system bridges this gap by providing digital IDs to all students, regardless of their socioeconomic status.

10.1 Contributions to the local and global economy development

The Educational ID system is designed with inclusivity in mind, catering to diverse student needs, including those with disabilities or residing in remote areas. By removing physical barriers and ensuring accessibility, the system fosters equal opportunities for every student, promoting an inclusive and equitable learning environment.

10.2 Impact on workforce productivity and skill development

By addressing socioeconomic inequality, the IOG Digital ID system promotes increased educational attainment. Empowered with digital credentials, students pursue higher education and improve their prospects for social mobility. This, in turn, positively impacts the economic development of the country, as a well-educated workforce drives economic growth.

10.3 Enhancing employability and reducing unemployment rates

10.3.1 Verifiable credentials for employers

The Educational ID system provides employers with a transparent and verifiable way to validate applicants' qualifications and achievements. This reduces hiring cycles, minimizes the cost of background checks, and enhances recruitment efficiency. Employers confidently make hiring decisions, knowing that candidates possess the requisite skills and qualifications.

10.3.2 Fostering entrepreneurship and innovation

A skilled and qualified workforce, empowered by the Educational ID system, is more likely to pursue entrepreneurship and innovation. As aspiring entrepreneurs embark on business ventures, they drive economic growth, create job opportunities, and contribute to technological advancements in various industries.

10.4 Contribute to financial inclusion

10.4.1 Access to educational funding

Digital IDs streamline the process of accessing educational funding, scholarships, and grants. Students from diverse socioeconomic backgrounds benefit from financial assistance, reducing the barriers to entry and increasing Educational attainment rates.

10.4.2 Integration with financial services

The Educational ID system is integrated with financial services, offering students access to banking facilities, savings accounts, and financial literacy programs. This integration fosters financial inclusion, empowering students to make informed financial decisions and build a strong foundation for their future.

The implementation of an Educational ID system goes beyond improving administrative efficiencies in education; it brings about substantial external economic benefits. By contributing to local and global economic development, empowering the workforce, enhancing employability, and promoting financial inclusion, this system paves the way for a more prosperous and inclusive society. Educational institutions, policymakers, and stakeholders are encouraged to embrace this transformative technology, recognizing its potential to unlock economic opportunities and foster a sustainable future.

11. Cost of non-adoption

In an era marked by rapid technological advancement, educational institutions face a critical decision regarding the adoption of innovative solutions. Among these, the implementation of a digital ID system stands as a pivotal choice that significantly influences an institution's efficiency, security, and reputation. Failing to embrace this transformation results in substantial costs and consequences that extend far beyond the immediate operational scope. This section examines the potential losses in efficiency, security, and reputation that educational institutions could face if they opt not to implement a digital ID system.

11.1 Losses in efficiency

Institutions that continue to rely on traditional paper-based identification methods expose themselves to a range of inefficiencies. Manual processes, such as recording attendance, managing library access, and distributing resources, is time-consuming and error-prone. Without the automation and streamlined workflows that a digital ID system offers, valuable staff hours are expended on administrative tasks that could otherwise be directed towards higher-value activities like teaching, research, and student support. This inefficiency impedes the institution's overall productivity and hinders its ability to adapt to the evolving demands of modern education.

11.2 Compromised security

One of the most pressing concerns for any educational institution is maintaining a secure and safe environment for its members. Without a robust digital ID system, the risk of identity fraud, unauthorized access, and breaches of sensitive data increases. Traditional identification methods are susceptible to counterfeiting and unauthorized duplication, potentially leading to fraudulent individuals gaining access to the institution's premises or resources. Such security breaches compromise the safety of students, faculty, and staff, erode trust within the institution, and even lead to legal consequences in cases of data breaches.

11.3 Tarnished reputation

In the digital age, an institution's reputation is intricately tied to its ability to embrace and implement technological advancements. Failure to adopt a digital ID system projects an image of stagnation and unwillingness to adapt to the changing landscape. This

perception could deter prospective students, faculty, and partners who seek institutions that prioritize security, efficiency, and modernity. A negative reputation is challenging to overcome, affecting not only student enrollment but also funding opportunities, partnerships, and collaborative endeavors.

11.4 Missed opportunities for personalization

Modern education is increasingly focused on personalized learning experiences that cater to individual needs and preferences. Without a digital ID system, institutions miss out on the opportunity to seamlessly integrate personalized services and platforms. These systems provide tailored learning content, recommendations, and support, enhancing the overall Educational journey for students. The lack of personalization could lead to disengagement and hinder student success.

The cost of non-adoption of a digital ID system in educational institutions extends beyond mere financial considerations. The inefficiencies, compromised security, tarnished reputation, and missed opportunities for personalized learning collectively create a significant deficit that impacts the institution's long-term viability. To remain competitive, relevant, and responsive to the demands of the digital age, embracing a digital ID system is not merely a technological upgrade but a strategic imperative that paves the way for enhanced efficiency, security, and overall educational excellence.

12. Conclusion

The solution presented in the current document has been fully deployed at the Ministry of Education in Ethiopia.

A journey towards higher education is undergoing a paradigm shift, and the integration of digital educational credential systems is leading the way. This transformative step not only simplifies the transition to higher education but also streamlines transfer procedures, nurtures comprehensive educational records, and integrates universities into a holistic digital ecosystem. The benefits of this transition are both profound and far-reaching, reshaping the landscape of education and beyond.

As students embark on their higher education journeys, the digital educational credential system eases their path. Tedious administrative processes and convoluted transfer procedures are replaced with seamless digital interactions. This fosters a more conducive learning environment, allowing students to focus on their academic pursuits rather than bureaucratic hurdles.

A hallmark of this digital transformation is the empowerment of students to create and maintain a thorough record of their continuous education. From academic achievements to skill development, every milestone becomes a part of their digital portfolio. This holistic representation equips students with a **tangible demonstration of their growth, fostering confidence and readiness for the challenges of the future.**

Unlocking a world of opportunities: The integration of universities into the digital educational credential system marks a monumental stride. Educational institutions become interconnected nodes within a network of learning and growth. This collaborative approach paves the way for standardized recognition, enabling students to navigate diverse educational paths with ease.

The benefits of this digital transformation ripple beyond the confines of academia. It addresses pervasive challenges faced by educational institutions worldwide, saving precious time, conserving resources, and enhancing overall efficiency. This efficiency

contributes to the acceleration of the digital economy, allowing institutions to redirect resources toward innovation and meaningful student experiences.

In an era where trust and authenticity are paramount, the digital educational credential system stands as a **bastion against fraud**. Credentials stored thanks to secure blockchain technology offer a **tamper-proof record of achievements**. This fosters an environment of credibility, where employers and institutions can verify accomplishments with confidence.

The most empowering aspect of this transition lies in its **direct impact on employment and job creation**. Graduates armed with comprehensive digital credentials possess a competitive edge in the global job market. This translates to meaningful employment opportunities and contributes to the growth of industries and economies.

In conclusion, the integration of universities into the digital educational credential system signifies not just a technical innovation but a holistic transformation of educational pathways. **This innovation empowers students, optimizes institutions, supports the digital economy, and safeguards authenticity**. It is a step towards a future where learning is truly recognized, transitions are smooth, and opportunities are abundant. Embarking on this journey means embracing the potential to redefine education for generations to come.

Annex 1: List of illustrations

Annex 2: Useful reference links

1. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech-2022 **McKinsey Technology Trends Outlook 2022**
2. https://unesdoc.unesco.org/ark:/48223/pf0000386147**: Global Education monitoring report summary, 2023: technology in Education: a tool on whose terms?**
3. https://blogs.worldbank.org/edutech/new-research-hub-use-technology-Education-developing-countries **A new research hub on the use of technology in Education in developing countries**
4. **UNESCO Institute for Statistics. (2019). Education in Sub-Saharan Africa: Facts and Figures.** http://uis.unesco.org/sites/default/files/documents/fs51-Education-africa-en-2019.pdf**.**
5. **EMIS framework** http://wbgfiles.worldbank.org/documents/hdn/ed/saber/supporting_doc/Background/EMIS/Framework_SABER-EMIS.pdf
6. **How is technology shaping the future** https://www.edsurge.com/research/guides/how-is-technology-shaping-the-future-of-k-12-Education
7. **Leveraging and securing data for Education** https://www.ecampusnews.com/resource-library/leveraging-and-securing-data-for-Education/
8. **Role of government in Education**

   https://www2.deloitte.com/us/en/insights/industry/public-sector/role-of-government-in-innovation.html
9. **Student Information System Market Report, 2022-2030,** UNESCO EMS

Annex 3: Contact

IOG Singapore Pte. Ltd.
4 Battery Road
#25-01 Bank of China Building
Singapore (049908)
https://iohk.io/en/contact/