ANEXO 2 - GUIA PARA LA PRESENTACIÓN DEL PROTOTIPO CON EL QUE SE POSTULA EL EQUIPO

Bogotá, 4 de septiembre 2019

Señores:
Fundación Tecnalia Colombia - Apps.co Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC
Bogotá D.C.

Asunto: Presentación del prototipo con el que se postula el equipo a la convocatoria RetoLab_ Reto Blockchain

Respetados señores, la presente tiene como fin, presentar los elementos que conforman el prototipo con el que se está postulando el equipo multidisciplinario denominado **Linking Data** a la convocatoria de RetoLab, Reto:-Blockchain:

1. **Nombre del equipo: Linking Data**
2. **Título del proyecto: Sistema Blockchain para la gestión de Certificados de conceptos de interés público: Hyperledger-Fabric y Python, trabajando juntos para garantizar interoperabilidad.**
3. **Resumen ejecutivo y palabras clave**

Un certificado representa una afirmación expresada por un emisor y asociada en algunos casos a un receptor. Las tecnologías blockchain proporcionan un conjunto de medios que permiten la trazabilidad, seguridad y permanencia de la afirmación en su conjunto u atomizada. Para el emisor y receptor la tecnología habilita otros aspectos que marcan una diferencia con respecto a los certificados físicos o digitales alternativos. Por ejemplo, la posibilidad de revocar o expirar el certificado una vez emitido por parte del emisor.

El prototipo a desarrollar propone el diseño de un sistema de gestión de Certificados de conceptos de interés público, la construcción de los componentes esenciales y la articulación entre estos. El sistema está compuesto por: la definición de estándares de certificación, las historias de usuario y diseños apropiados, una aplicación de emisión para blockchain permisionado, diseño de red permisionada para entidades públicas, y un validador universal (independiente e interoperable) para diferentes tipos de blockchain.

Palabras Clave: Hyperledger, Fabric, Composer, Blockcerts, OpenCerts, Credenciales Verificables, Blockchain permisionado, Blockchain no permisionado, Python.

4. **Descripción de la solución:**

La solución requiere el diseño del modelo de datos que definen un certificado, junto con la especificación de los procesos relacionados al ciclo de vida del certificado. El primer caso permite definir un estándar para la estructura de la información contenida en el certificado y los mecanismos de seguridad que permiten posteriormente hacer una validación de los contenidos. En el segundo caso la definición de los procesos nos permite organizar las

aplicaciones y componentes del sistema, teniendo en cuenta los objetivos de interoperabilidad.
Los certificados desde una definición amplia son una convención social a partir de la cual es posible visibilizar un nuevo conjunto de información, usualmente una afirmación que como mínimo involucra un emisor. Las tecnologías actuales de emisión de certificados son físicas, mediante papel, y digitales que utilizan mecanismos de seguridad y validación centralizados a través de los sistemas de firmas digitales.

Los certificados físicos o digitales contienen una estructura de la información: afirmación o nueva información, descripción del emisor, identificación del receptor (opcional) y unos mecanismos de seguridad (firma, fecha, entre otros). Por el otro lado el ciclo de vida de un certificado consiste en una emisión, visibilizar o compartir el certificado emitido a través de un canal de comunicación, y verificación de la información contenida de manera conjunta o en algunos casos de algunos componentes específicos y significativamente más relevantes dentro de la afirmación.
Las tecnologías blockchain proporcionan a los certificados digitales los siguientes valores agregados:

1. Permanencia y trazabilidad.
2. Verificación independiente.
3. El emisor cuenta con un mecanismo seguro y sin costos adicionales para revocar o darle caducidad a la afirmación una vez emitida.
4. El receptor controla su información y por lo tanto complementa los modelos de identidad auto-soberana.
5. Proporciona una red amplia y no excluyente de compartir la información con bajas probabilidades de censura o manipulación versus in sistema centralizado de gestión de la información.
6. Remplaza la necesidad de contar con un sistema de administración centralizado de firmas digitales, por un validador universal que consulta la red blockchain.

No todos estos beneficios se pueden o se deben adoptar de manera simultánea. Teniendo esto en cuenta, proponemos un sistema que en una primera etapa únicamente se enfoque en la afirmación (conceptos de interés público) y el emisor, dejando para un desarrollo posterior un rol activo para el receptor. Es decir, en nuestro caso de uso el receptor asume un rol pasivo y por lo tanto lo podemos incorporar en caso de ser necesario dentro de la información o afirmación contenida en el certificado.
Ya existen casos de uso implementados para la emisión de certificados académicos que reflejan diferentes niveles de titulación a nivel de educación superior o educación para el trabajo. Quizás el modelo más conocido es el estándar Blockcerts, desarrollado por MIT y Machine Learning en 2015 y que ha sido exitosamente implementado y utilizado para emitir y verificar certificados utilizando la red Bitcoin y Ethereum. El proyecto propone un estándar (*schema*) o modelo de datos y unos componentes (*end-to-end*) de: emisión (*cert-tools, cert-issuer*), verificación (*cert-verifier*), visualización (*cert-viewer*) y portabilidad (*wallet*) que encapsulan una parte importante del ciclo de vida de los certificados académicos. En el año 2018, fuimos los primeros en proponer la utilización del estándar en redes permisionadas mas precisamente utilizando Hyperledger Fabric y Composer, por esta razón fuimos invitados a presentar este trabajo en el Hyperledger Global Forum 2018.

El diseño técnico de la solución está basado en los siguientes componentes y plan de trabajo:

1. Explorar el tipo de certificados emitidos por entidades públicas para tener unos marcos de referencia.
2. Definición de un estándar o schema en dos niveles: primero la información contenida en el certificado (*Cert-Schema:* afirmación y emisor) localizado *on-chain* o preferiblemente *off-chain* en un registro administrado por cada una de las entidades públicas; segundo la abstracción del certificado (*Abstraction-Schema*: identificador, localización, campos de verificación) localizado *on-chain* en un registro de gobernanza compartida (Diagrama 1).
3. La lógica de negocio de emisión y verificación se prueba mediante una prueba de concepto auto contenida en una blockchain permisionado utilizando Composer-Playground.
4. Experiencia e interfaces de usuario para el emisor (entidades del sector público). Generar plantillas que a nivel de diseño visual faciliten la interacción entre usuario y máquina, haciendo que estas brinden los elementos gráficos (por ejemplo, campos de información) necesarios para registrar la información que constituirá la base de datos de los certificados, evidenciando las etapas de construcción de la información para que el usuario tenga conocimiento de la fase del procedimiento en que se encuentra. Concepto central a trabajar: formulario y un paginador para indicar fase o etapa de la información registrada.
5. Experiencia de usuario y opciones para el verificador universal. De la misma manera que en el emisor, a nivel de diseño gráfico el reto es crear un entorno de consulta que sea de fácil comprensión con el objetivo de facilitar no solo la verificación de la información sino el entendimiento de los resultados de los mismos buscando que la experiencia pueda ser satisfactoria para el usuario. Este entorno visual se centrará en la idea de una caja de búsqueda de resultados y el despliegue de sus resultados.
6. Despliegue de la lógica de negocio de Composer para emisión en Hyperledger Fabric y la implementación de un Frontend para emisión, habilitando la funcionalidad para usuarios (Diagrama 2).
7. Validador Universal en Python que por línea de código se integre con el registro de la red permisionada de Fabric para validar un certificado emitido (Diagrama 3).
8. Propuesta de validador universal en Python que interactúe con la red Ethereum.
9. Propuesta de la arquitectura de una red permisionada con Hyperledger Fabric para la emisión de certificados en entidades públicas (Diagrama 4).
10. Por último la solución plantearía una incorporación paulatina de los nodos y los retos de pasar del prototipo en Composer a la solución en producción utilizando los contratos inteligentes (chaincode) programados utilizando golang y Hyperledger Fabric (Chaincode API).

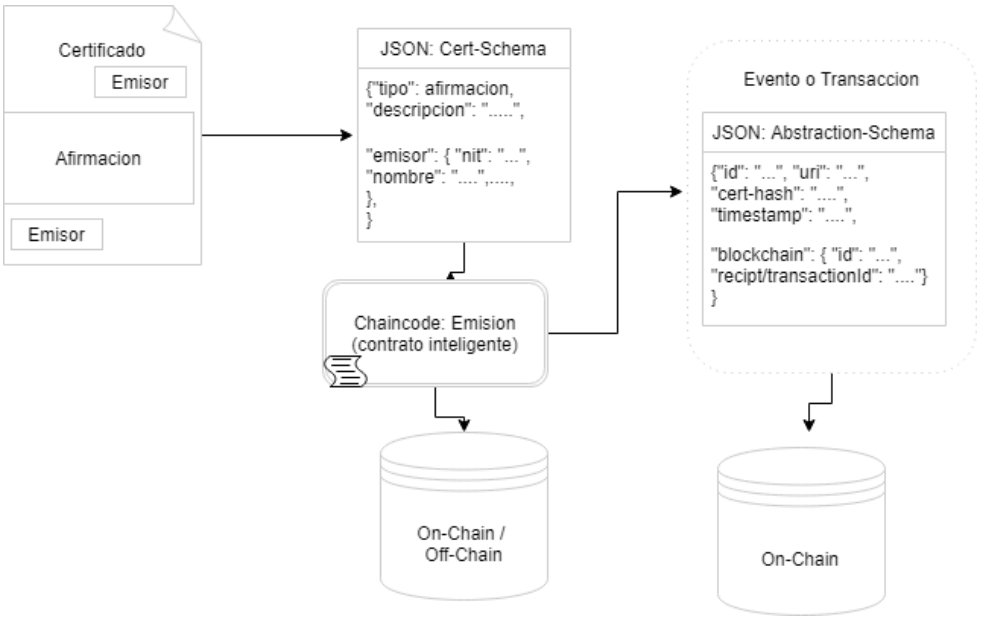

Diagrama 1: Proceso de emisión de un certificado

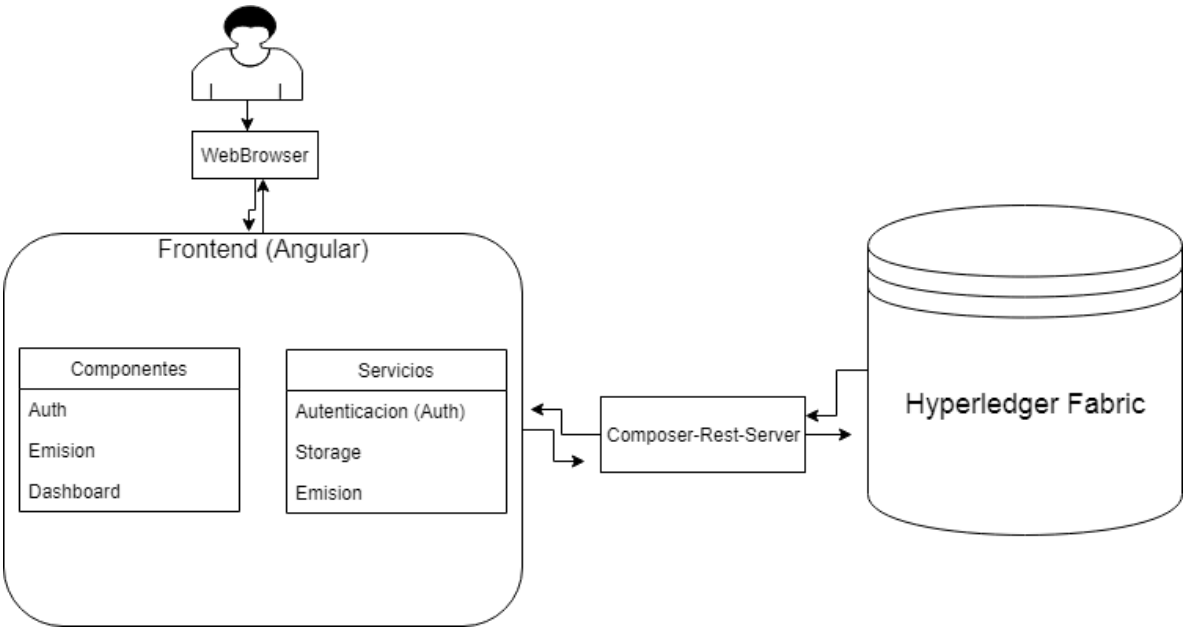

Diagrama 2: Arquitectura aplicación Emisor red permisionada

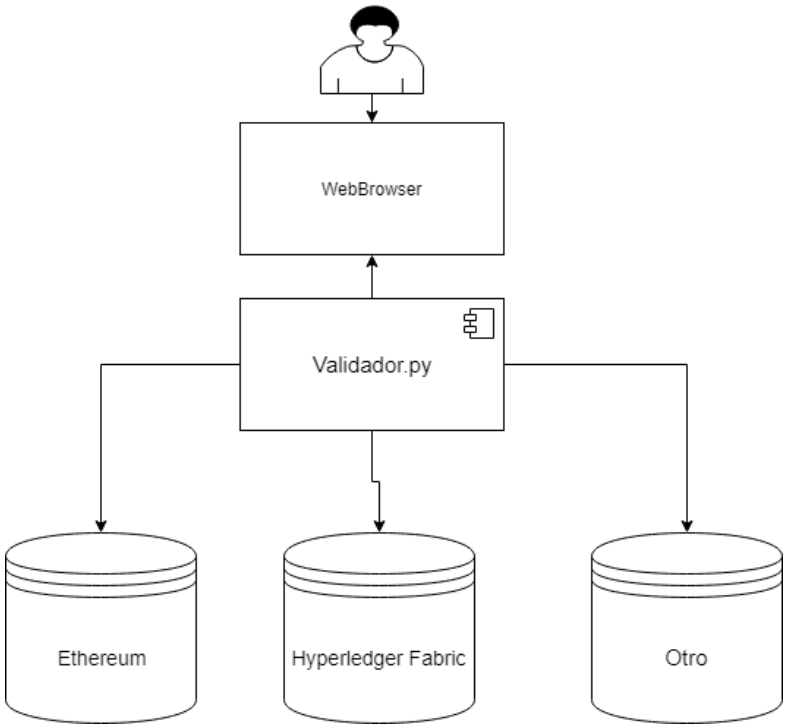

Diagrama 3: Arquitectura aplicación Validador General

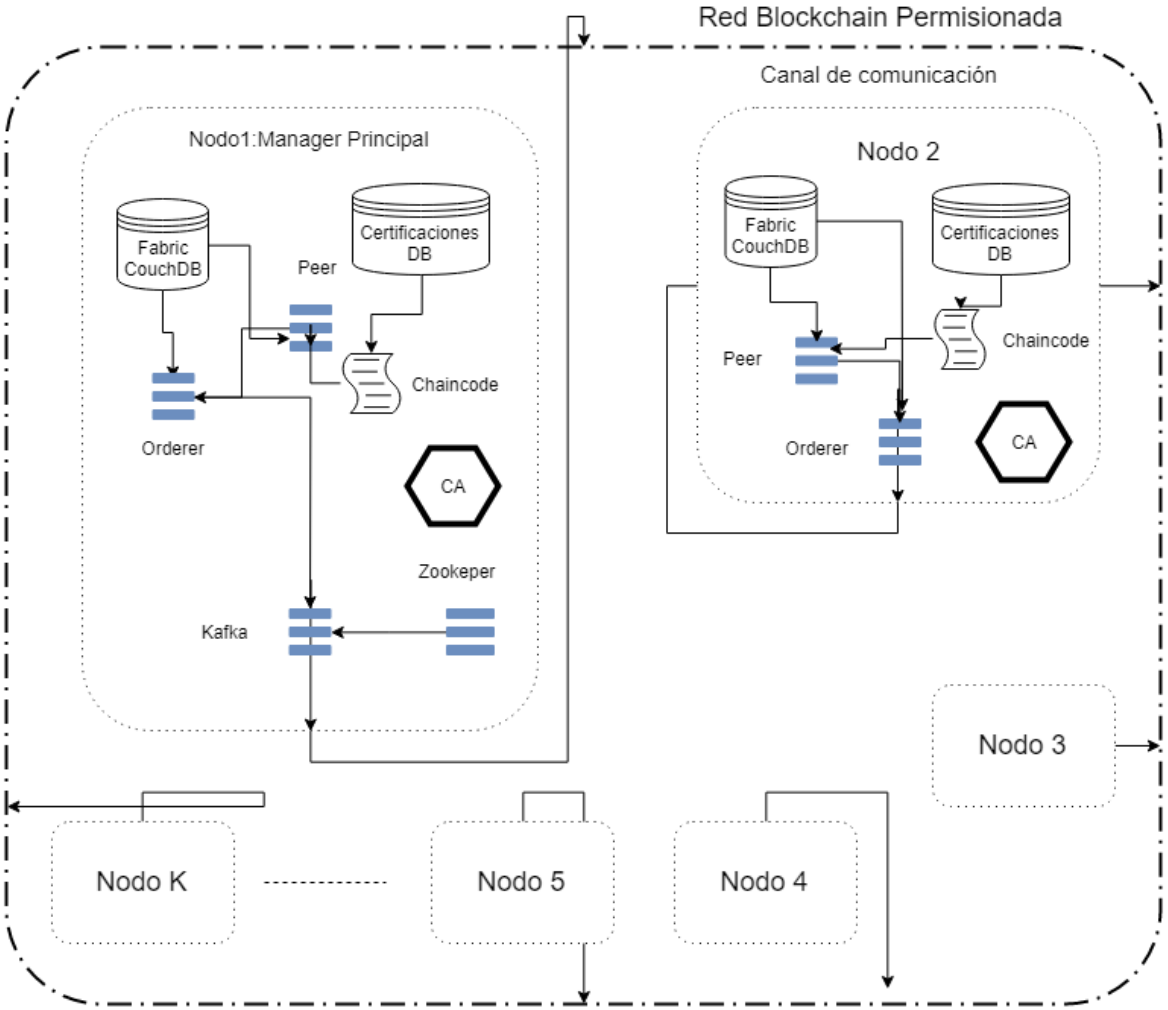

Diagrama 4: Arquitectura red permisionada entidades públicas (escalable)

De acuerdo a las aplicaciones que se mencionan en el plan de trabajo, nuestras estrategias con respecto a la experiencia de usuario y el diseño de las interfaces de usuario tienen las siguientes consideraciones:

- Ha de ser un diseño limpio, con tipografía y elementos visuales que se complementan y responden a los parámetros visuales dispuestos por las entidades para formularios que recolectan información y respetando la identidad visual de las mismas. Sabemos que la interfaz y la experiencia de usuario se correlacionan y depende una de la otra, es por esto que al entender que la experiencia de usuario es orgánica la interfaz lo reflejará, ya que a medida que los usuarios interactúen con la plataforma nos darán las directrices para mejorar dicha experiencia haciendo que la interfaz se adapte a los requerimientos del usuario y el entorno haciendo que el diseño evolucione.

- Proponemos que para el ambiente de emisor el diseño se enfoque en equipos de escritorio (desktop), siendo la medida estándar 1366 x 768 px, pues es la pantalla más usada actualmente. En el caso del verificador, el diseño partirá del concepto *first mobile*, ya que consideramos que el verificador debe ser asequible desde cualquier dispositivo móvil para facilitar la consulta y obtención de información, en este caso la medida es 640 x 360 px y a partir de este adaptarlo a dispositivos como tablets y pantallas de escritorio.

4.1 Estado de avance del prototipo.

En los proyectos desarrollados en los últimos dos años tenemos una experiencia importante en diferentes aplicaciones para la emisión y validación de certificados educativos y la trazabilidad de objetos de investigación. Todos estos proyectos están contenidos en la el repositorio oficial de la organización Blockchain4openscience. Algunos de estos componentes son un marco de referencia para los componentes a desarrollar pero ninguno cumple la finalidad exacta del reto por lo tanto el trabajo a desarrollar es totalmente nuevo. En las próximas semanas y antes de la Hackathon lograremos avanzar en los puntos 1 al 3 del plan de trabajo mencionado anteriormente; discutir los desafíos y viabilidad de la arquitectura, la experiencia de usuario y los componentes que estamos proponiendo dentro del equipo.

Lo avances se pueden observar en el repositorio oficial del equipo: https://github.com/linkingdatasas/RetoApps

5. Indique por qué se considera que el prototipo es innovador, indicando las características específicas diferenciadoras de otras propuestas existentes en el mercado.

El prototipo sigue las propiedades de estándares de certificados educativos (en donde tenemos experiencia y donde hemos aportado al uso en blockchain permisionada) y los adapta al caso de emisión de conceptos por parte de entidades del sector público. La propuesta es conservadora y realista en su alcance, y por lo tanto simplifica el modelo de datos para enfocarse en la afirmación y el emisor. Adicionalmente, proporciona una solución integral e interoperable al incorporar componentes de redes permisionadas desde el proceso de emisión y proponiendo un validador universal que este en la capacidad de verificar emisiones de certificados en blockchain permisionado y no permisionado. Esto es posible por el diseño una estructura de datos en dos niveles; el primero que contiene la información completa del certificado (off-chain) y la segunda una capa ligera de asociación (ubicación) y seguridad que se encuentra en el blockchain. Por último, la propuesta incluye un plan de implementación modular y escalable mediante el cual nodos de diferentes entidades públicas se puedan incorporar a la red permisionada independientemente de las características específicas de los certificados emitidos por cada entidad y por lo tanto evitando dificultades en la rápida adopción de la tecnología. Como un objetivo adicional y de carácter opcional se puede explorar la necesidad de compartir la información contenida en los certificados y de relevancia interinstitucional para concebir canales privados para que las entidades públicas compartan la información.

Nota: *Con la firma del presente documento declaro que la información contenida en ésta corresponde a la realidad y que mi firma es autógrafa. En consecuencia, asumiré la plena responsabilidad en el evento de presentarse alguna inconsistencia que pueda inducir a error.*

CARLOS ALBERTO CASTRO-IRAGORRI

C.C. 79.947.917

LIDER DEL GRUPO