La identidad autosoberana como solución descentralizada a la custodia de credenciales privadas

Self-Sovereign Identity as a decentralized solution to the custody of private credentials

Autor: Marcos Hidalgo Baños

Tutor: Isaac Agudo Ruiz

Cotutor: Rodrigo Román Castro

Tiempo estimado de exposición: 20 minutos

Fecha designada para la defensa: 24 de Septiembre de 2024

Análisis de aplicabilidad

1) Introducción al paradigma.
2) Ámbitos de implementación.
    a) Identidad Digital Europea
    b) Internet de las Cosas
    c) Gemelos Digitales
3) Reflexiones personales.

Prueba de Concepto

1) Definición de los componentes del sistema.
2) Características técnicas.
3) Valoración general.
    a) Limitaciones y aspectos a mejorar
    b) Dificultades encontradas

Etapas definidas en el Anteproyecto del TFG

Fase inicial de investigación

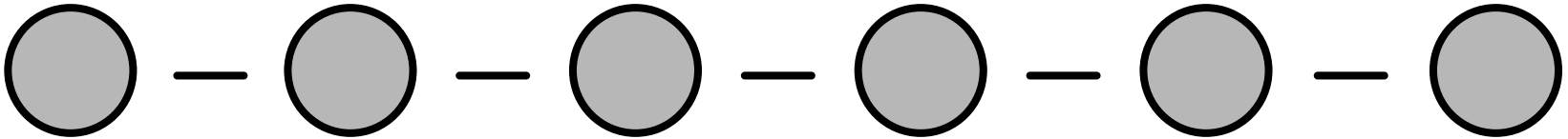
Creación de las pruebas de concepto

Comparativa con la normativa europea

Valoración general

Redacción de la memoria

Elaboración de la presentación



Análisis de aplicabilidad

1) ***Introducción al paradigma.***
2) Ámbitos de implementación.
    a) Identidad Digital Europea
    b) Internet de las Cosas
    c) Gemelos Digitales
3) Reflexiones personales.

¿Qué propone la Identidad Autosoberana?

Una novedosa **alternativa** a la tradicional manera *centralizada* para la gestión de credenciales.

Identidad

- Los usuarios poseerán las **credenciales** en sus dispositivos.
- Estas se almacenarán en las **Carteras de Identidad Digital**.

Autosoberana

- No necesitar de terceras partes, **empoderando** al usuario.
- Emplear tecnologías **descentralizadoras** como la Blockchain.

Actores y sus funciones en el paradigma

- **Emisor.** Es el encargado de **generar** y firmar las credenciales pedidas por los usuarios. Este rol puede ser tomado por entidades gubernamentales, corporaciones e individuos.

- **Titular.** Es el usuario que **dispone** de sus credenciales y las almacena en su Cartera de Identidad Digital. Representa a todo portador de Identidad Digital, de cualquier naturaleza.

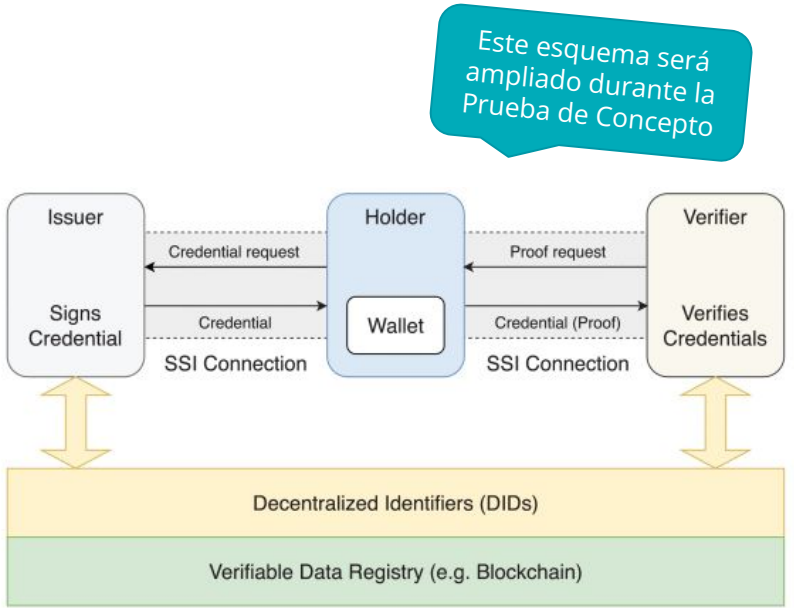
- **Verificador.** Recibe y procesa las credenciales para **comprobar** su validez. Representan a aquellos interesados en verificar la identidad de los Titulares, como las instituciones o negocios.

Actores y sus funciones en el paradigma

Observación relevante

Un **mismo** actor es capaz de adquirir las funciones de otros.

La **imparcialidad** y **confianza** depositadas en las credenciales se verán notablemente afectadas.



Identificadores Descentralizados (DIDs)

- **Esquema.**

  Definido como ‘did’, representa el esquema de identificación a seguir.

- **Método DID.**

  Indica la implementación a utilizar para la resolución del DID.

- **Identificador específico.**

  Permite asociar inequívocamente al usuario dentro del método en cuestión.

Credenciales Verificables (VCs)

- **Afirmaciones.** [obligatorio]

  Relación establecida entre el sujeto y el valor asignado mediante la propiedad que se describe.

  Ejemplo: el autor de esta presentación **(sujeto)** es alumno **(propiedad)** de la UMA **(valor)**.

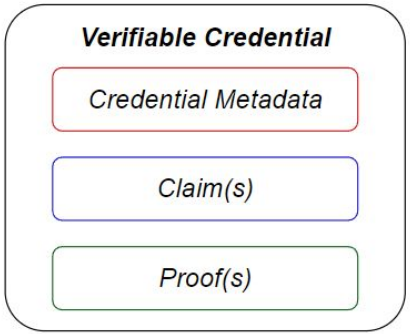
- **Metadatos.** [opcional]

  Descriptores de aspectos de la credencial (fecha de expiración).

- **Pruebas.** [opcional]

  Datos criptográficos que determinan al emisor (firma digital).

Sólo son verificables si se especifica este apartado



Credenciales Verificables (VCs)


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://university.example/credentials/3732",
  "type": ["VerifiableCredential", "ExampleDegreeCredential"],
  "issuer": {
    "id": "https://university.example/issuers/565049",
    "name": "Example University",
    "description": "A public university focusing on teaching examples."
  },
  "validFrom": "2015-05-10T12:30:00Z",
  "name": "Example University Degree",
  "description": "2015 Bachelor of Science and Arts Degree",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "ExampleBachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
}
```


Observación relevante

El Titular puede **seleccionar** información de diferentes credenciales para **combinarlas** en un mismo entregable de tamaño reducido mediante una **Presentación Verificable**.

Análisis de aplicabilidad

1) Introducción al paradigma.

2) Ámbitos de implementación.

- ***a) Identidad Digital Europea***
- ***b) Internet de las Cosas***
- ***c) Gemelos Digitales***

3) Reflexiones personales.

¿Qué supone la Identidad Digital Europea?

Infraestructura Europea de Servicios Blockchain (EBSI)

¿Qué supone la Identidad Digital Europea?

Establecer el paradigma de la Identidad Autosoberana a los **ciudadanos** y **empresas** europeas.

eIDAS Bridge

- Comprobar si una determinada credencial verificable tiene **validez** para ser empleada en la Unión Europea.
- Asistir a los Emisores durante el **firmado** de la credencial y a los Verificadores con la **identificación** del DID del Emisor.

Cartera(s) de Identidad Digital Europea

Cada país miembro debe implementar una aplicación móvil siguiendo el **estándar**.

La Identidad Autosoberana en el Internet de las Cosas

Red de Confianza Integrada (ITN)

El término **Certificado Verificable** para los objetos puede ser entendido como el equivalente de **Credencial Verificable** para las personas.

La ITN “actúa” como el **Registro de Datos Verificables**

Concepto interesante

Gemelo Digital Autosoberano (SSDT)

Ámbitos de trabajo en un entorno de Gemelos Digitales

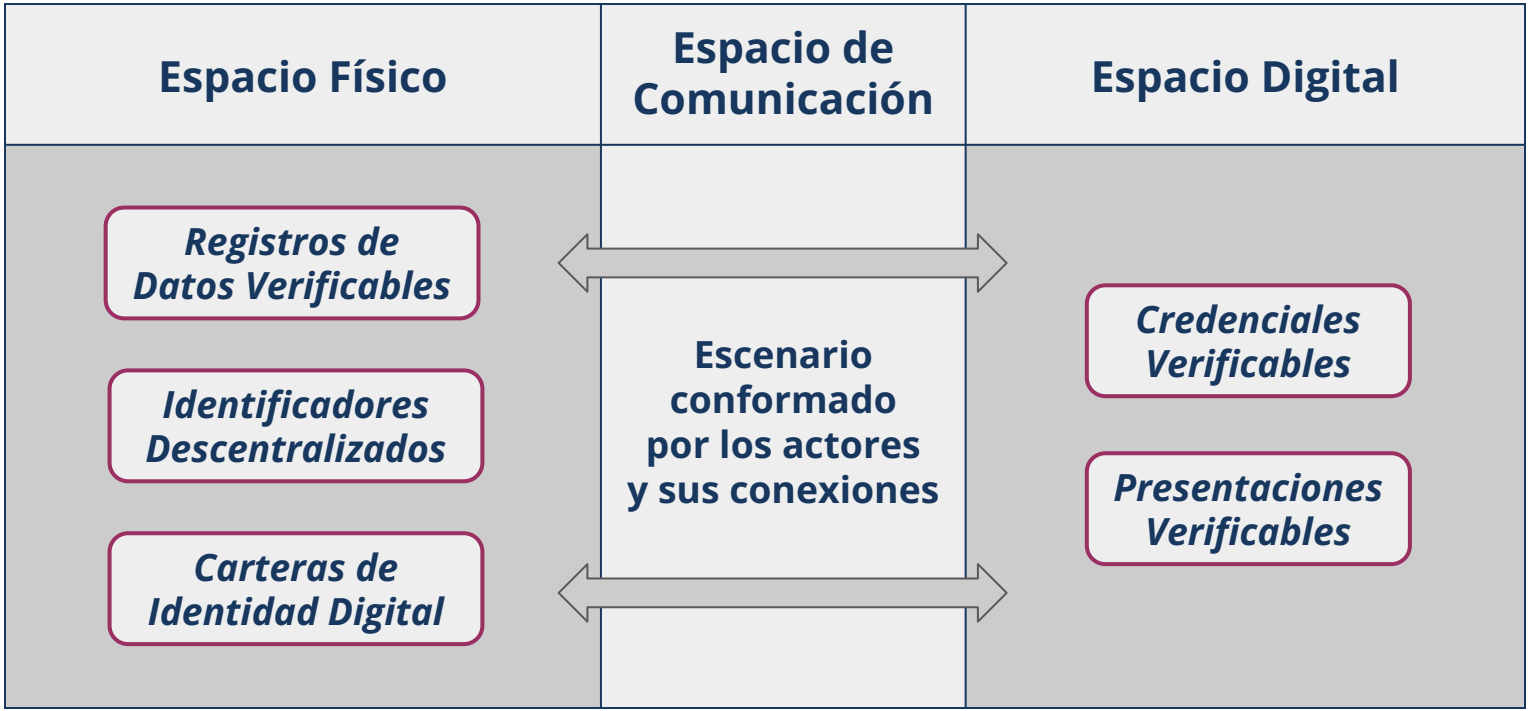


Tabla resumen del análisis realizado

	Aspecto vulnerado	Riesgo SSI intrínseco	Amenazas DT relacionadas	Amenazas DT mitigadas
Capa 1	VDR	R1.1	A1.1, A1.2	A1.3
	Cartera de Identidad Digital	R1.2 R1.3	A1.4 A1.6, A1.7, A1.8	A1.5 No aplican
Capa 2	Nodo de la red	R2.1	A2.1, A2.2, A2.3, A2.4	A2.5
	Comunicaciones	R2.2	A2.6, A2.7, A2.8	No aplican
Capa 3	VC	R3.1	A3.1, A3.2, A3.3	A3.4
Capa 4	Representación	R4.1	A4.1, A4.2	A4.3

Es más fácil atacar el Espacio **Físico** y de **Comunicación** que el **Digital**

Las principales vulnerabilidades surgen entre la capa 1 y 2

Los mecanismos técnicos de la Identidad Autosoberana mitigan algunas amenazas

Análisis de aplicabilidad

1) Introducción al paradigma.
2) Ámbitos de implementación.
    a) Identidad Digital Europea
    b) Internet de las Cosas
    c) Gemelos Digitales
3) Reflexiones personales.

Conclusiones elaboradas tras el estudio

- Sobre el paradigma de la **Identidad Autosoberana**.

Alternativa a la centralización

Fortalezas:

- Robustez criptográfica.
- Objetivo descentralizador.

Flaquezas:

- Problemas de escalabilidad.
- Uso malicioso de los mecanismos técnicos del paradigma, como la Cartera de Identidad Digital.

Críticas al diseño de las funciones de los actores

El Titular **no** puede formar parte del sistema si no es mediante el Emisor.

Esto se debe a que es el único actor capacitado para incluir **transacciones** en el Registro de Datos Verificable.

La Credencial Verificable necesita la **firma** del Emisor para ser válida.

Conclusiones elaboradas tras el estudio

- Sobre el establecimiento de la **Identidad Digital Europea**.

Dificultades legales para su implantación

Derecho al olvido:

- El Registro de Datos Verificables no permite la eliminación de transacciones ya efectuadas.

Reglamento General de Protección de Datos (GDPR):

- Las Credenciales Verificables constituyen la Identidad Digital.

Europa como líder regulador en tecnología

La Comisión Europea ha destacado por llevar la **iniciativa** global en la regulación de nuevas tecnologías.

Aunque puede llegar a **perjudicar** su correcto desarrollo e implementación, Europa ejerce una excelente labor de **tutelaje** mediante sus recursos legislativos y financieros.

Prueba de Concepto

1) ***Definición de los componentes del sistema.***
2) Características técnicas.
3) Valoración general.
    a) Limitaciones y aspectos a mejorar
    b) Dificultades encontradas

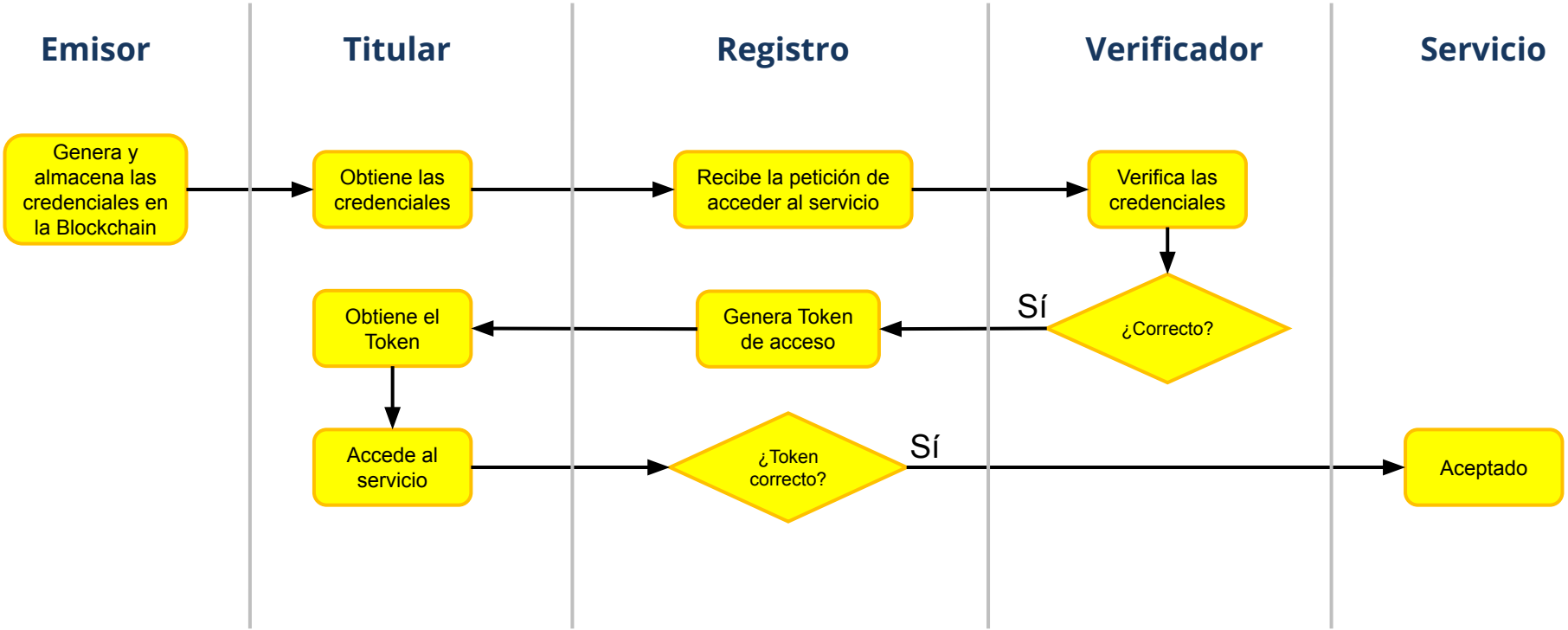
Nuevos actores añadidos para el sistema

- **Registro.** El Titular debe adquirir un **token** de control de acceso al Servicio que es expedido por este actor.
  Define un **diccionario** para asociar los DIDs a dichos tokens.

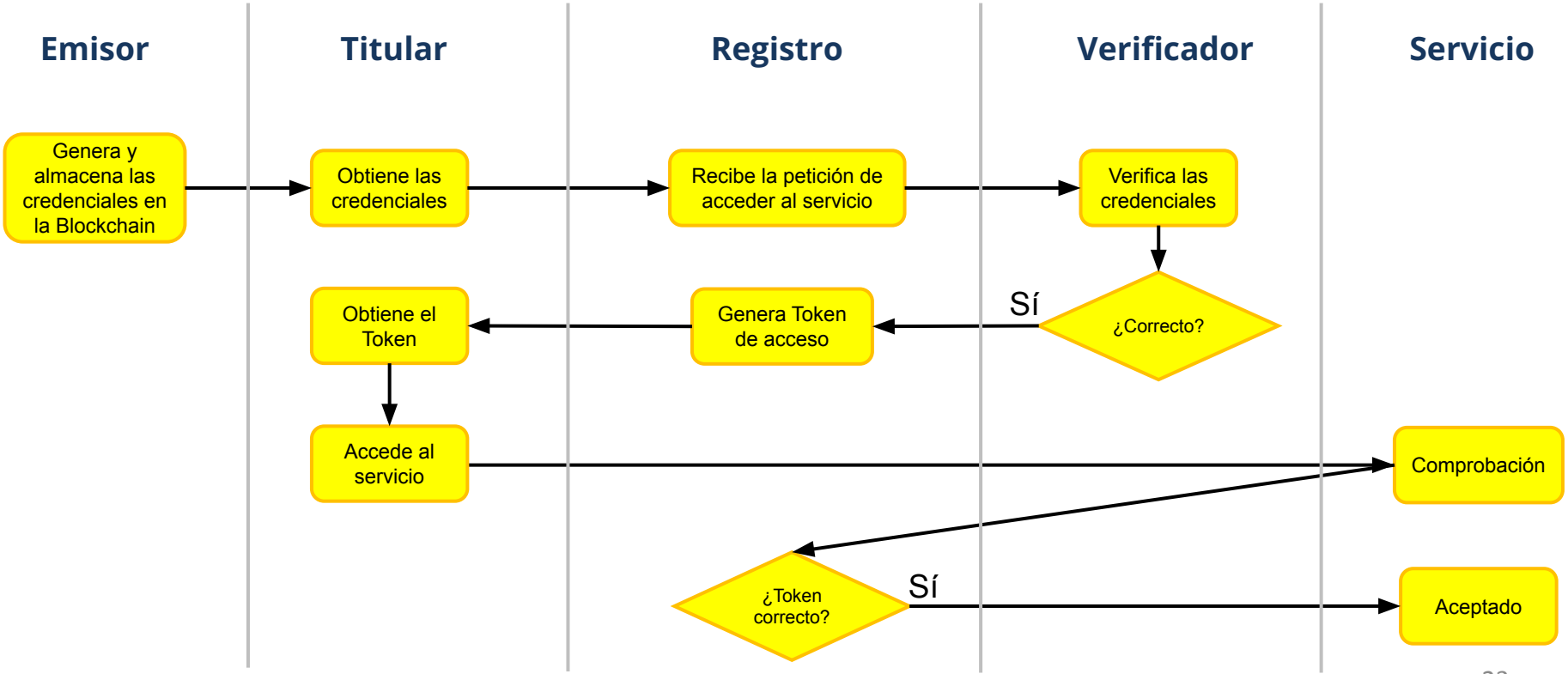
- **Servicio.** Representa el objetivo final del Titular, por el cual ha requerido de sus credenciales para identificarse.
  Realiza un **seguimiento** sobre los DIDs con acceso al mismo.

También se introduce un cuasi-actor denominado **main** que será el **monitorizador** del sistema. No es considerado parte de él ya que únicamente recibe y muestra los mensajes finales del Titular.

Flujo de acción [A] para la Prueba de Concepto



Flujo de acción [B] para la Prueba de Concepto



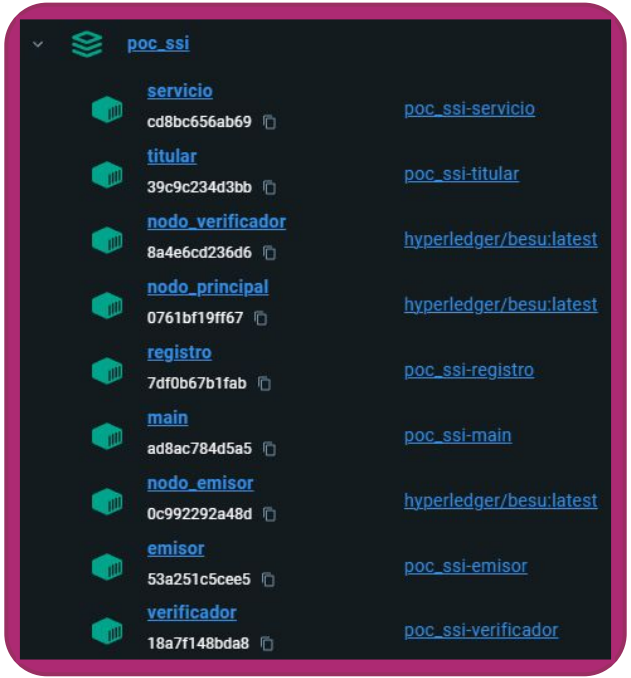
Prueba de Concepto

1) Definición de los componentes del sistema.

2) Características técnicas.

3) Valoración general.
   a) Limitaciones y aspectos a mejorar
   b) Dificultades encontradas

Instrucciones para ejecutar el sistema



El primer y único paso para ello es introducir el siguiente comando desde una terminal:

docker compose up -- build

Una vez efectuado, se permitirá al usuario monitorizar el sistema desde la dirección:

http://127.0.0.1:5000

Vídeo demostración

Prueba de Concepto

1) Definición de los componentes del sistema.
2) Características técnicas.
3) ***Valoración general.***
    a) ***Limitaciones y aspectos a mejorar***
    b) ***Dificultades encontradas***

Limitaciones y aspectos a mejorar del sistema

- **Ámbitos** sin explorar debido al **retraso temporal** ocasionado durante la Prueba de Concepto.

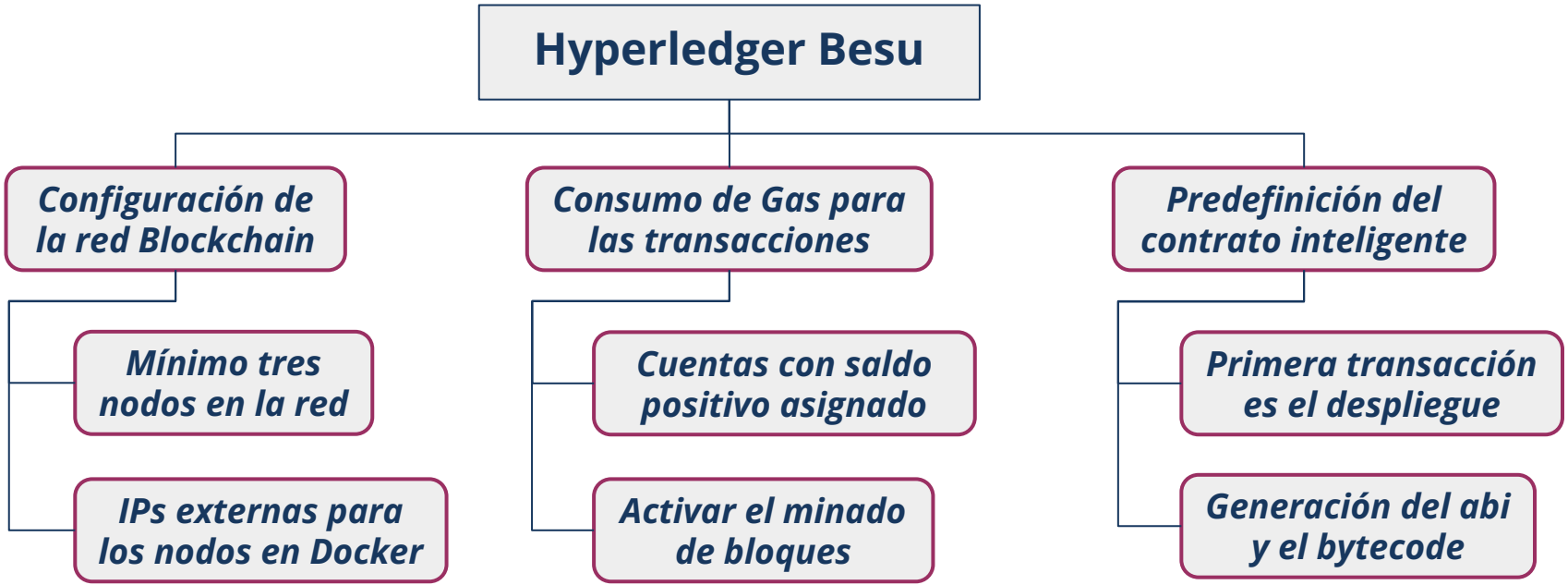
Inicialización relativamente lenta de la Blockchain

Volúmenes no definidos para los actores del sistema

El sistema no ha sido adaptado a Kubernetes

Las credenciales no incluyen la firma digital del Emisor

Dificultades encontradas durante la implementación



Balance individual para las etapas del TFG

Fase inicial de investigación

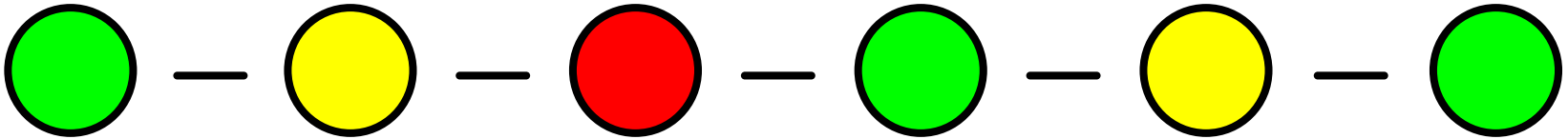
Creación de las pruebas de concepto

Comparativa con la normativa europea

Valoración general

Redacción de la memoria

Elaboración de la presentación



La identidad autosoberana como solución descentralizada a la custodia de credenciales privadas

Self-Sovereign Identity as a decentralized solution
to the custody of private credentials

Autor: Marcos Hidalgo Baños

Tutor: Isaac Agudo Ruiz

Cotutor: Rodrigo Román Castro

¡Gracias por su atención!