Middleware de seguridad para Blockchain en escenarios IoT

Autor
Alberto Robles Enciso

Directores
Dr. Antonio Fernando Skarmeta Gómez
Dr. Jorge Bernal Bernabé

Índice

- Motivación
- Objetivos
- Solución Propuesta
- Diseño de la solución
- Implementación
  - Dispositivo Personal
  - Dispositivo IoT
- Conclusiones
- Vías Futuras

Motivación

- El uso de la tecnología IoT trae consigo una serie de retos y dificultades, uno de los más importantes es la gestión segura de los datos que producen los dispositivos.
- Se tiene que ofrecer mecanismos de auditabilidad de la información almacenada (validación, integridad y procedencia) y también privacidad tanto en los datos (cifrándolos) como en la red de transacciones (blockchain con privilegios).
- Dentro de la red se deberá asegurar la identidad de los participantes por lo que es necesario ofrecer mecanismos para autenticarlos.

- Surge la necesidad de desarrollar sistemas que proporcionen capas extra de seguridad para solventar estos problemas.

Objetivos

- **Objetivo 1:** Estudiar que blockchain se usará y desplegarla.
- **Objetivo 2:** Desarrollar un mecanismo para generar transacciones.
  - **Objetivo 2.1:** Estudiar qué información almacenar en la transacción.
  - **Objetivo 2.2:** Estudiar donde guardar los datos que se envían.
- **Objetivo 3:** Estudiar como segurizar todo el proceso de comunicación y almacenamiento de datos.
- **Objetivo 4:** Diseño de la solución.
- **Objetivo 5:** Desarrollo de la solución.
  - **Objetivo 5.1:** Desarrollar una aplicación que realice estas tareas.
  - **Objetivo 5.2:** Desarrollar software de pruebas y un cliente web.
  - **Objetivo 5.3:** Pruebas de los clientes en equipos y dispositivos IoT.

Solución Propuesta

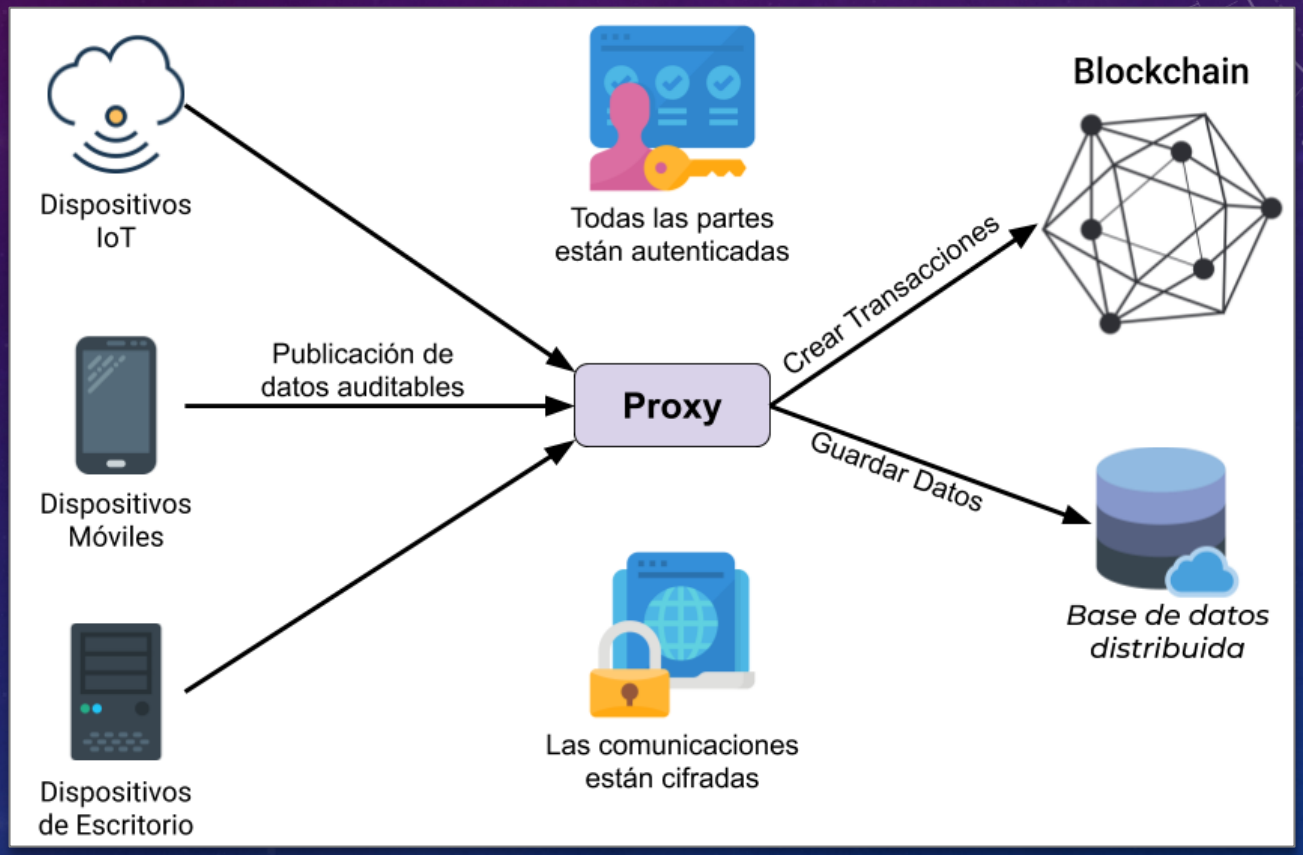
Se plantea, en base a las necesidades, el desarrollo de una plataforma que sirva como intermediario entre los clientes y la red IoT.

La plataforma, denominada **BSH** (Blockchain Security Handler), hará uso de la tecnología Blockchain para registrar la recepción de datos de forma segura y auditable. Además, hará uso de la red IPFS para persistir los datos cifrados de forma distribuida (offchain).

La blockchain que se usará será Hyperledger Fabric por tener un carácter empresarial, por ser privada y por no tener criptodivisa.

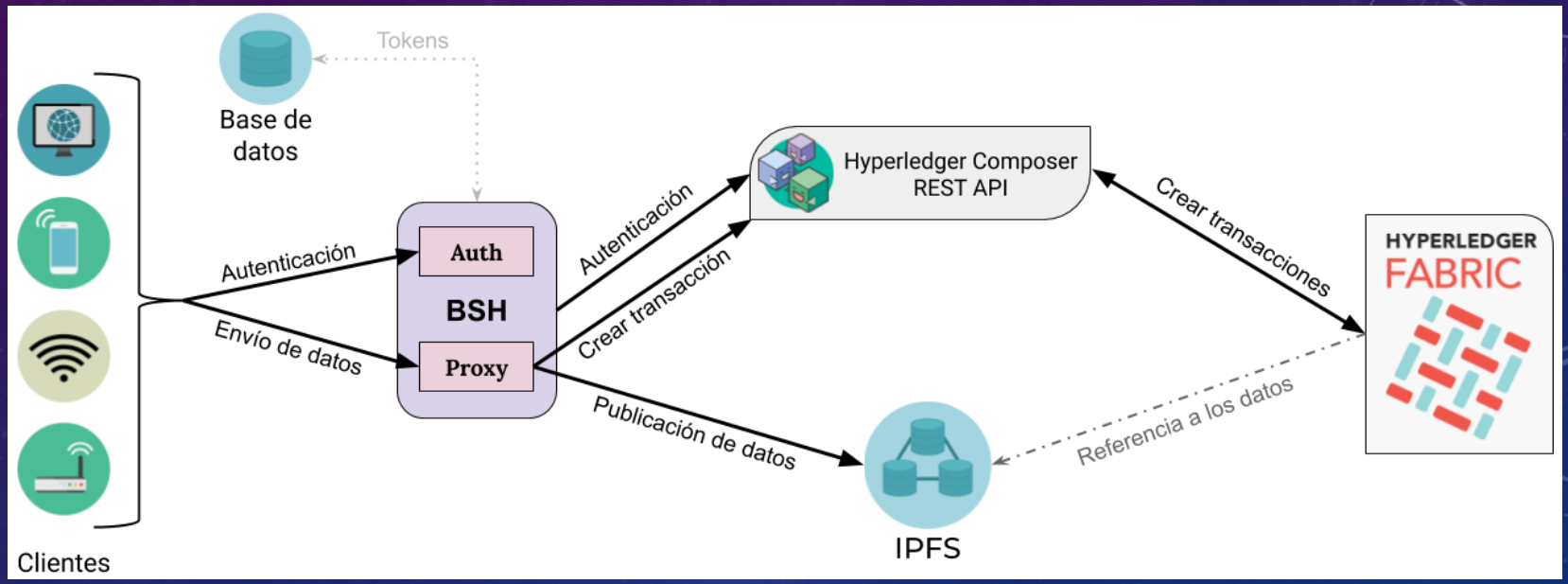
Solución Propuesta

Esquema simplificado



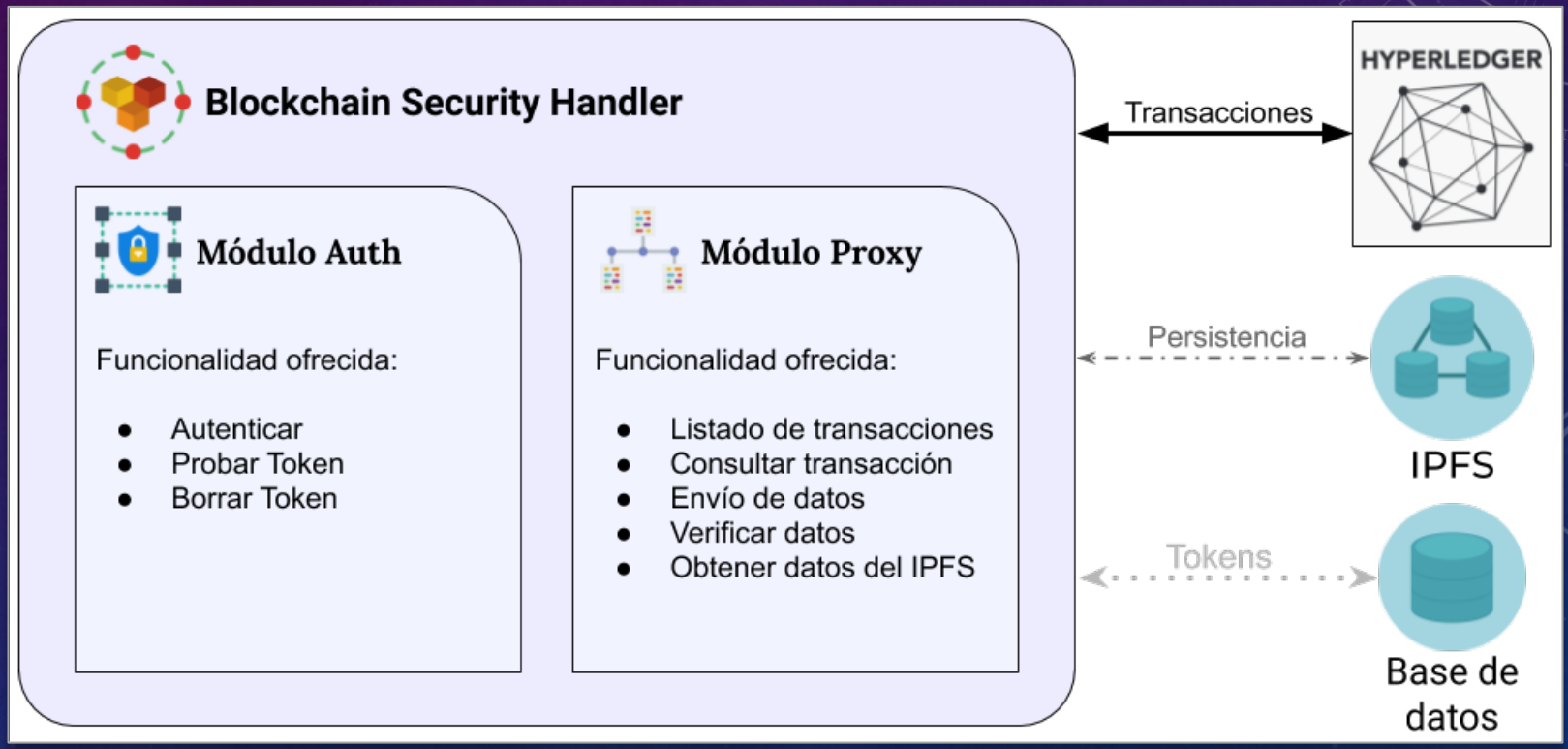
Solución Propuesta

Componentes del sistema



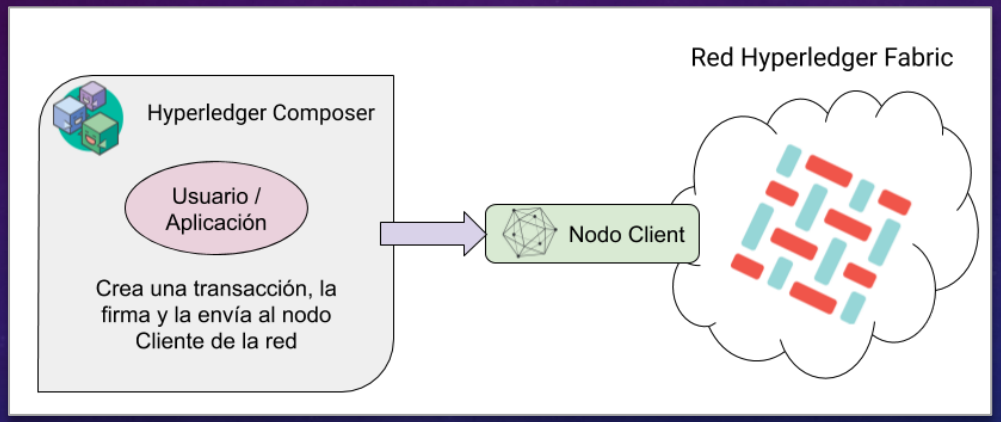
Solución Propuesta

Funcionalidad del BSH



Solución Propuesta

Hyperleder Composer y Fabric




```
namespace iot

transaction IoTTransaction {
  o String cid
  o String hash
  o String firmaAPI
  o String firmaUser
}
```

Diseño de la solución

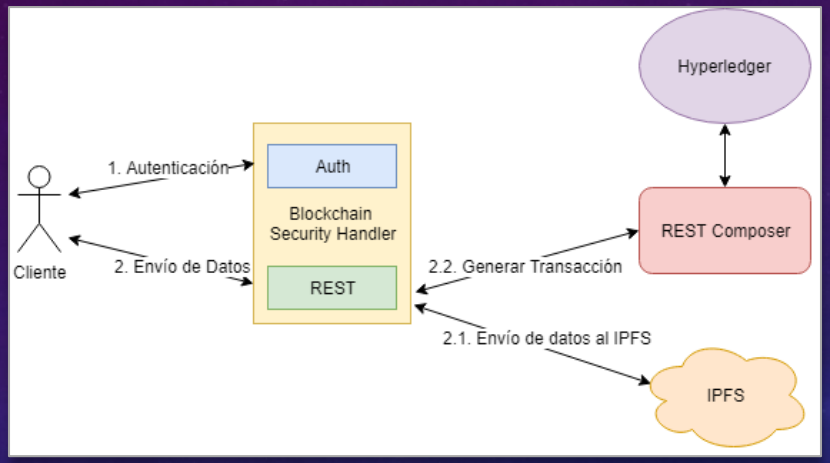
Para el mecanismo de autenticación surgen dos alternativas:

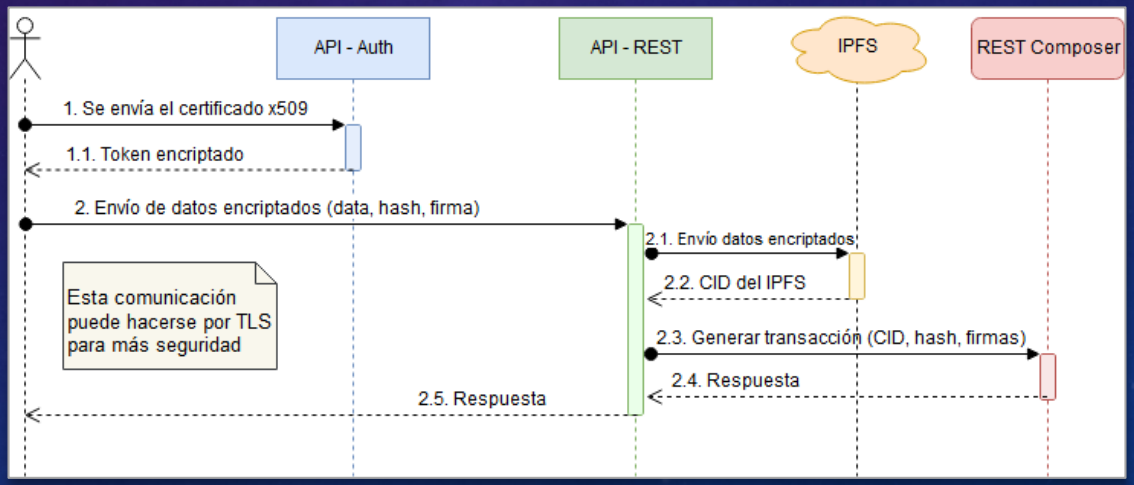
- **Autenticación centralizada**: El BSH realiza todo el proceso y gestiona las credenciales.

- **Autenticación federada**: El BSH delega el proceso a un sistema externo (FIWARE + eIDAS).

Diseño de la solución

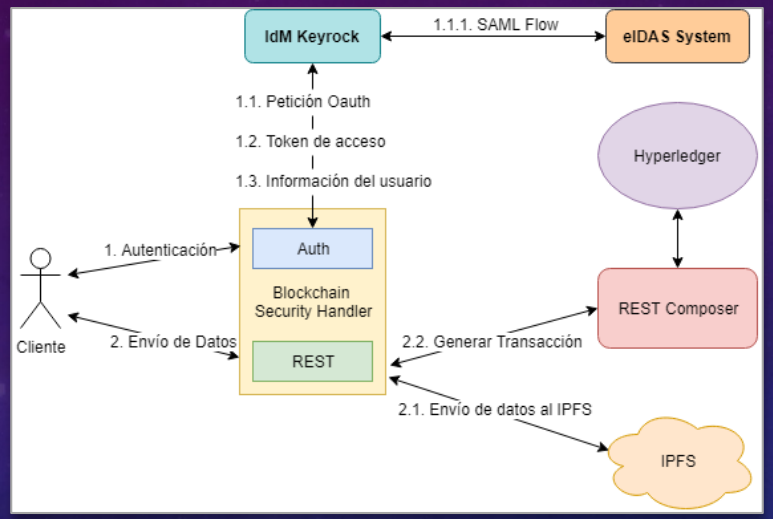
Esquema centralizado

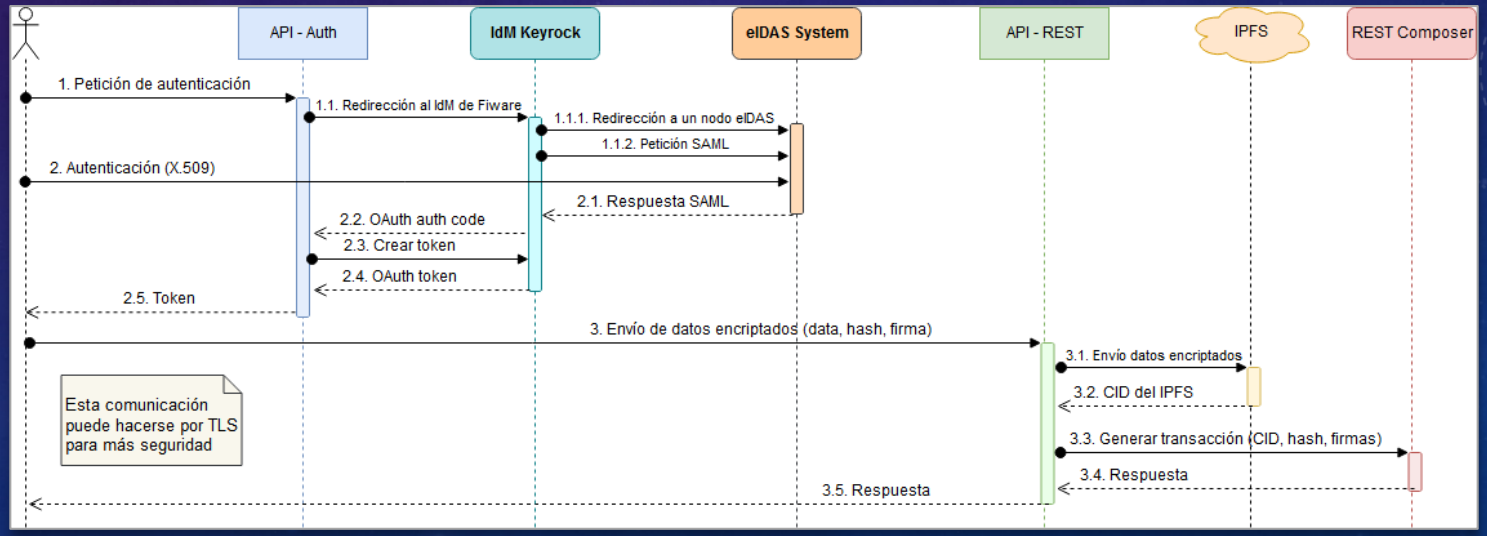




Diseño de la solución

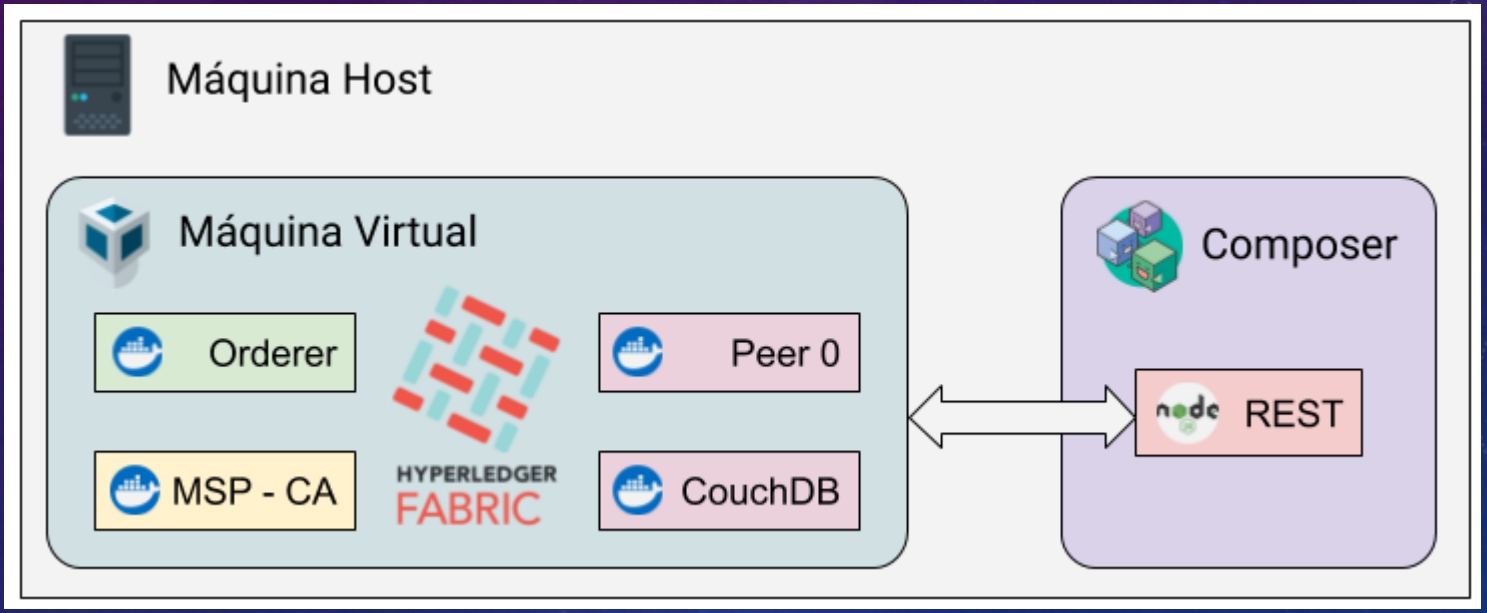
Esquema federado





Implementación

Despliegue Virtualizado



Implementación

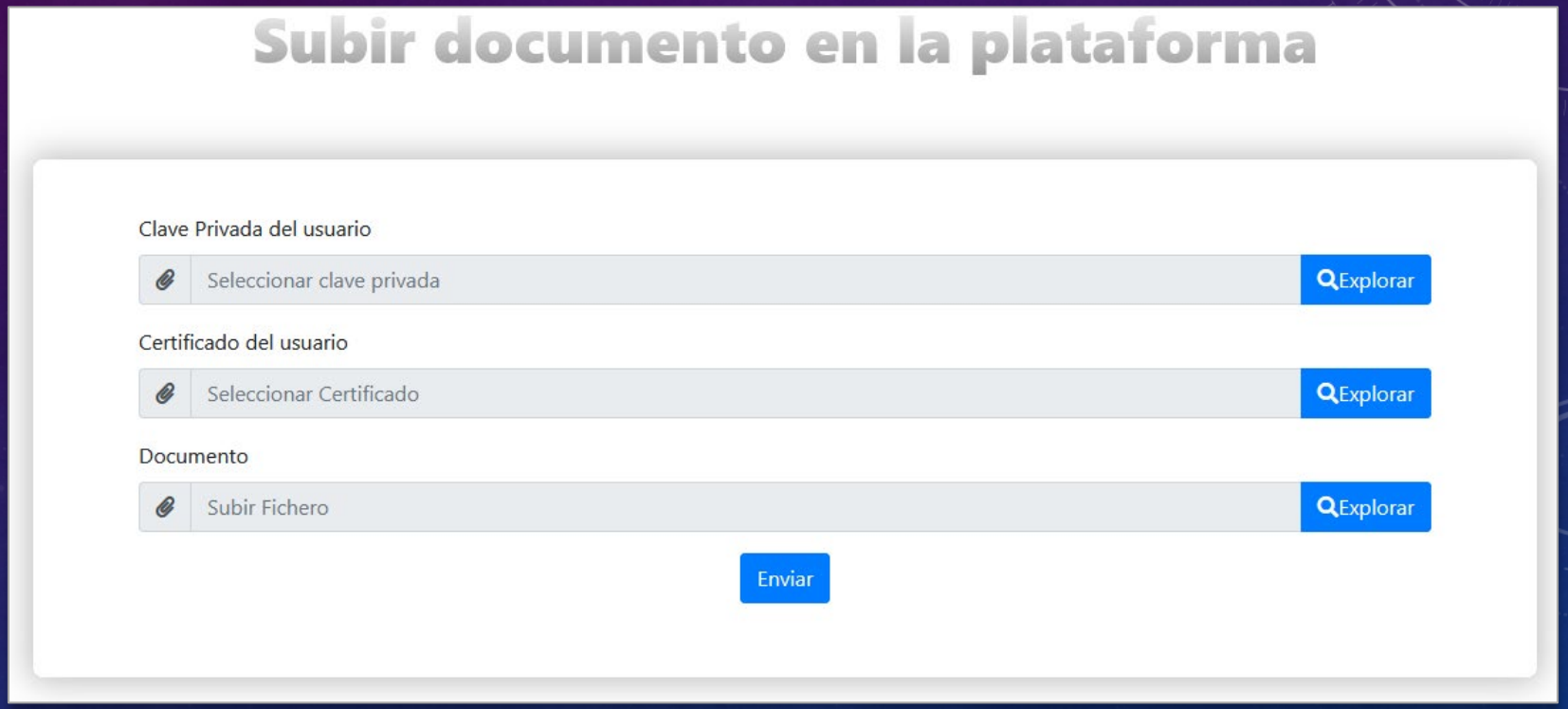
Clientes

Existen varios tipos de clientes (dispositivos IoT, moviles, ordenadores…), cada uno con unas necesidades concretas.

Para ejemplificar el uso de la plataforma por parte de estos clientes se diseñan dos casos de uso junto con el software que hará de cliente.

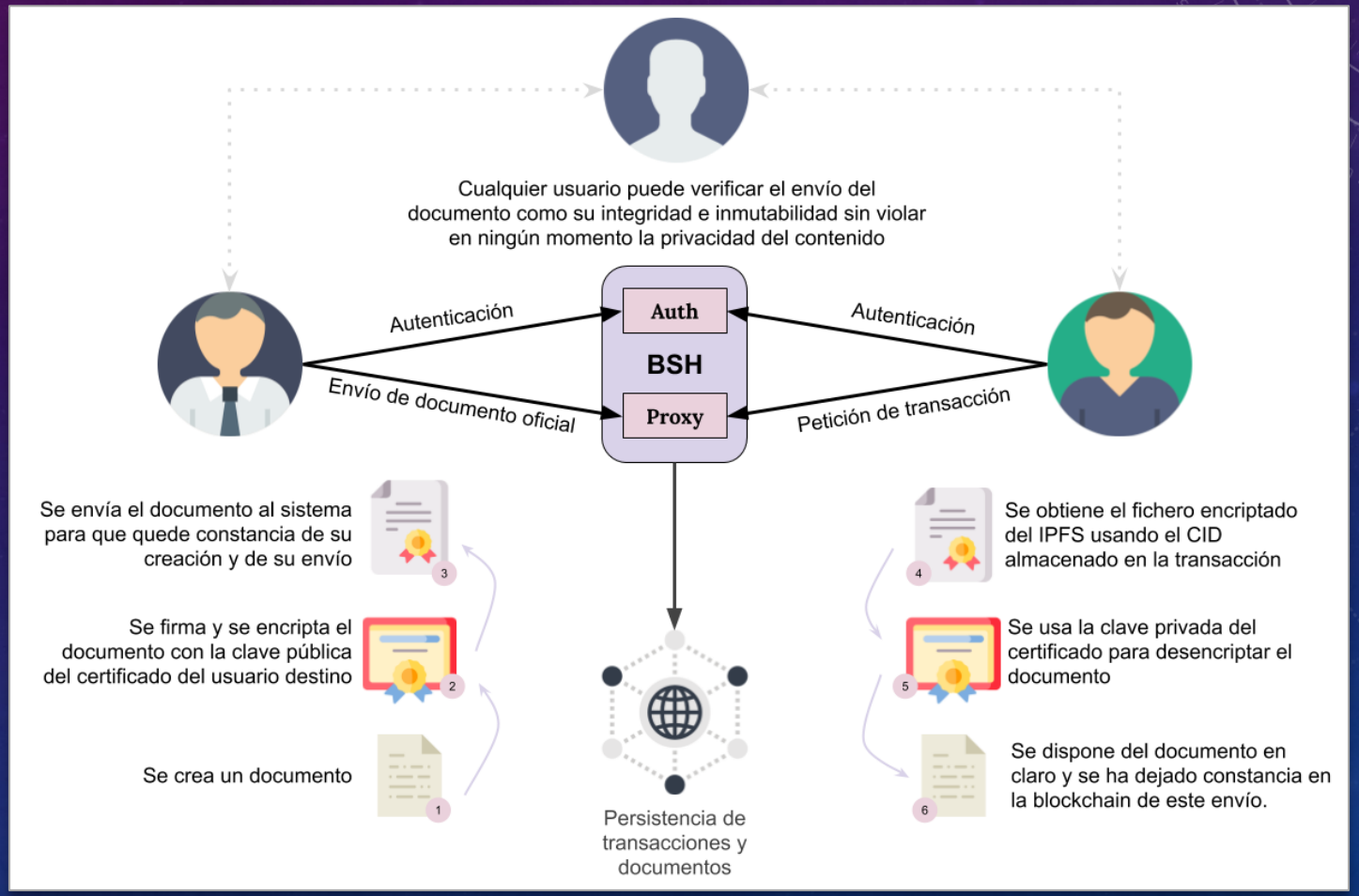
Cliente

Dispositivo Personal



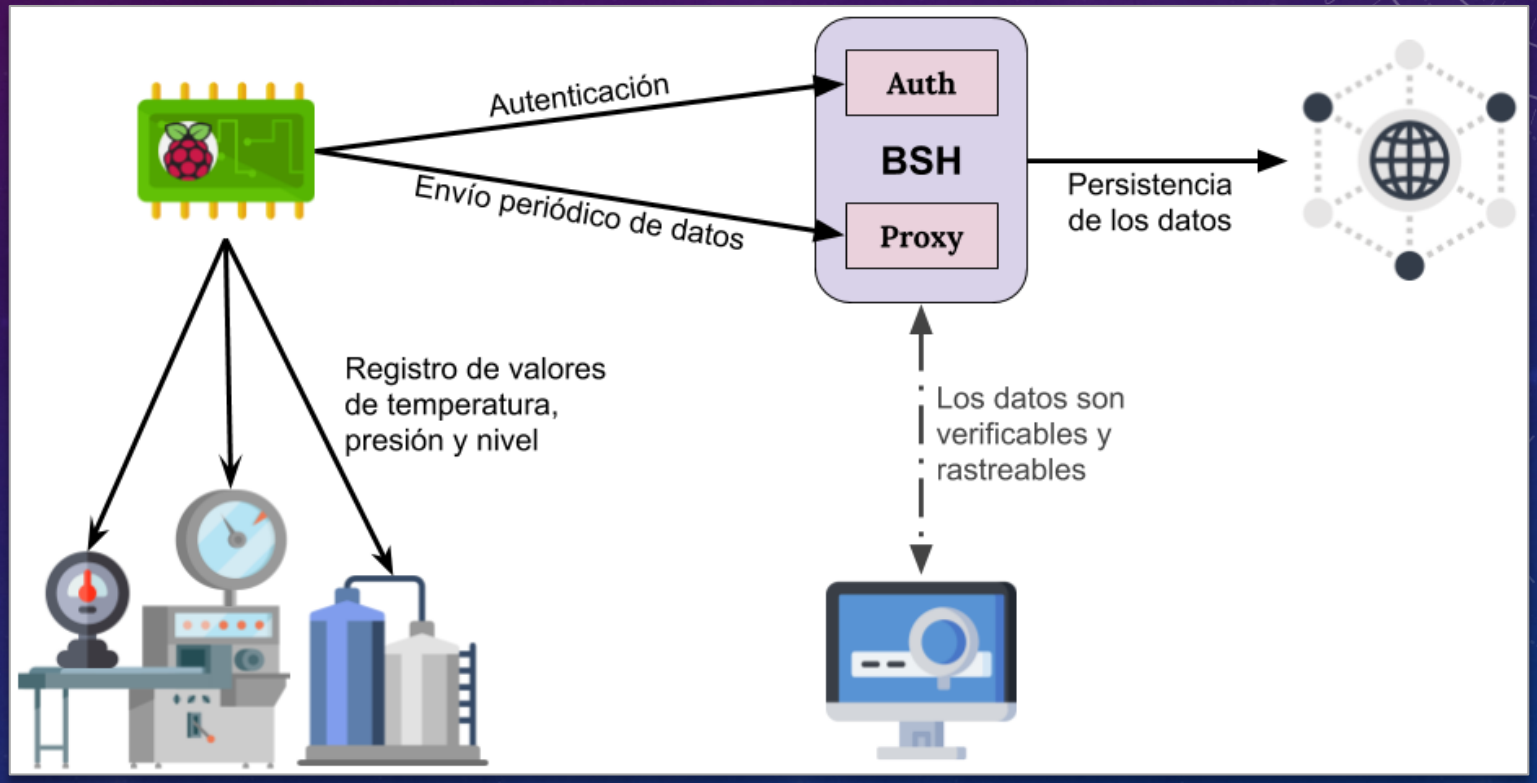
Cliente

Dispositivo Personal



Cliente

Dispositivo IoT



Conclusiones

Se ha logrado implementar una plataforma que sirve de PoC para añadir una capa de seguridad extra a una red IoT.

Se hace uso de tecnologías modernas como Blockchain e IPFS para lograrlo.

El diseño realizado es interoperable y fácilmente extensible a otras modalidades.

El trabajo se ha realizado en un contexto tecnológico de actualidad y en constante evolución.

Vías Futuras

- Realizar la implementación del esquema federado.
- Estudiar mecanismos de cifrados basados en políticas de atributos (CP-ABE).
- Realizar la autenticación mediante un Smart-Contract.
- Implementar el ejemplo del dispositivo Personal como un complemento del explorador.

Código Fuente

Todo el código desarrollado, los esquemas y los archivos usados están disponibles en el siguiente github:

https://github.com/alb1183/TFG/

Además, en el siguiente enlace se tiene un video que muestra un ejemplo de funcionamiento de la plataforma:

https://www.youtube.com/watch?v=fK0Qo9Wd-z4

Middleware de seguridad para Blockchain en escenarios IoT

Autor
Alberto Robles Enciso