Trabajo Práctico: Aspectos Legales de la Informática - Parte II

Universidad Nacional de la Patagonia San Juan Bosco

Blockchain Federal Argentina y Firma Digital en el Sistema Hospitalario de John Doe S.A

Alumno:

- Barea Matias Ezequiel

Profesores:

- Consentino, Guillermo
- Zappellini, Bruno

Introducción:

El presente informe tiene como objetivo explorar las posibilidades de integración de la Blockchain Federal Argentina y la firma digital en el sistema hospitalario de John Doe S.A. Esto permitirá mejorar la transparencia, seguridad, y cumplimiento normativo en la gestión de historias clínicas y documentos médicos.

Objetivo:

El objetivo de esta parte del trabajo práctico es familiarizarse con las tecnologías de firma digital y blockchain, comprender sus aplicaciones en el sector de la salud y cómo abordan desafíos legales y tecnológicos. A través de la exploración de estas tecnologías, los estudiantes podrán diseñar soluciones que cumplan con los requisitos legales y mejoren la seguridad e integridad de los datos médicos.

Firma Digital:

La firma digital es un método criptográfico que autentica la identidad del firmante y asegura la integridad del documento. Se basa en algoritmos de clave pública y privada. El firmante utiliza su clave privada para firmar electrónicamente el documento, y la clave pública se utiliza para verificar la autenticidad de la firma. Este proceso garantiza que el documento no ha sido alterado y que la firma es legítima.

Conforme la Ley 25.506, la firma digital cumple las mismas exigencias que la firma manuscrita de los documentos en papel, ya que posee las mismas características técnicas de seguridad que una firma en papel, e incluso mayores.

Esta cumple la función de facilitar el reemplazo de documentación en papel por su equivalente en formato digital. Ahorra costos, simplifica procedimientos y brinda seguridad en el intercambio de información. Se utiliza principalmente para firmar documentos PDF y correos electrónicos, pero también permite firmar documentos de texto, plantillas, imágenes y virtualmente cualquier tipo de documento. Su tecnología está incorporada en transacciones electrónicas, formularios web y navegación en páginas seguras.

Cómo funciona la firma digital:
La firma digital de un documento se obtiene tras una operación en tres pasos:

- Se aplica al documento un algoritmo matemático que crear una huella digital llamada hash. Este hash es un número que identifica de forma inequívoca el documento.
- El hash se encripta usando la llave privada del firmante.
- El hash encriptado y la pública del firmante se combinan en una firma digital que se agrega al documento.

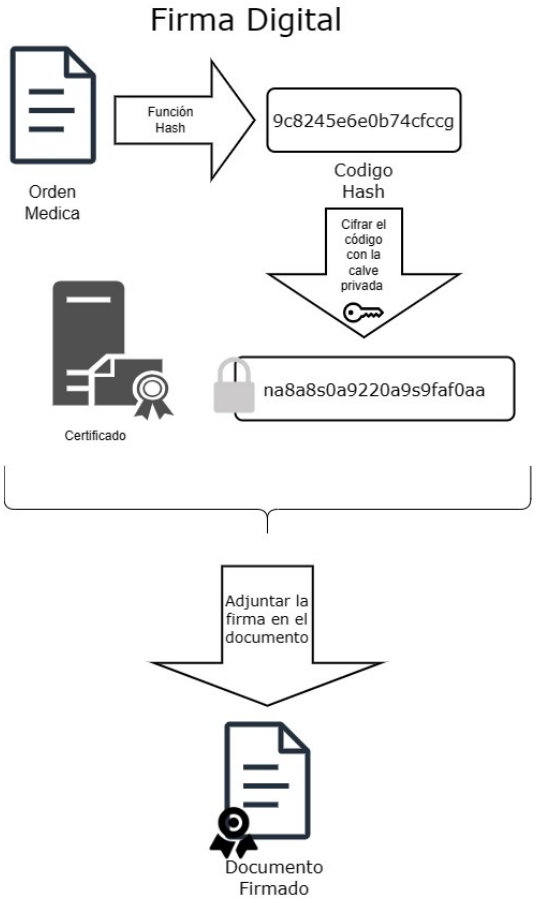
Para verificar la autenticidad del documento el receptor debe tener un programa que soporte firmas digitales. El programa usa la llave pública para desencriptar la clave hash. Luego calcula un nuevo hash para el documento. De este modo puede comparar el hash calculado con el hash desencriptado; si coinciden, el documento no ha sido modificado. Asimismo el programa valida que la llave pública usada en la firma pertenece al nombre que lo ha firmado.

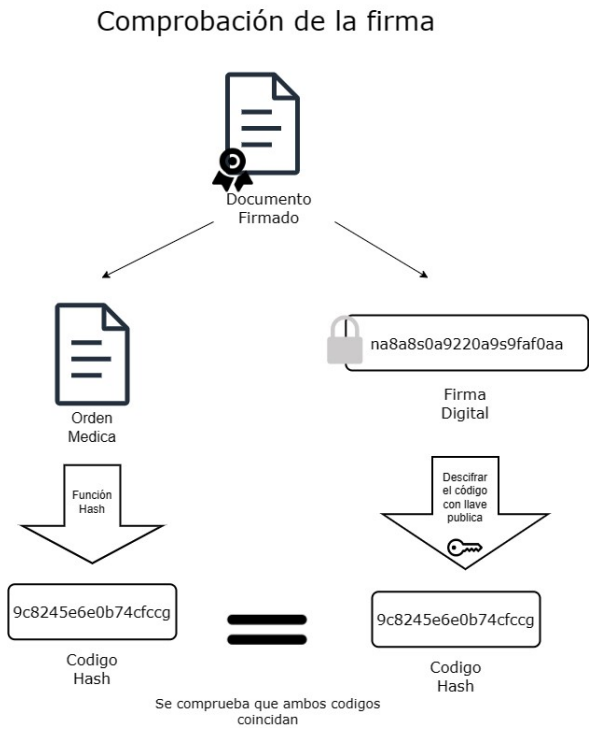
Casos de uso específicos:

La firma digital es utilizada dentro del contexto del sistema hospitalario para:

- **Historias Clínicas:**
  Cada historia clínica será firmada digitalmente por el médico responsable. Esto garantiza que cualquier modificación en el documento sea detectada, asegurando la integridad de la información médica. Además, la firma digital cumple con los requisitos legales para la validez de los documentos médicos.

- **Órdenes Médicas:**
  Las órdenes médicas también se firmarán digitalmente, asegurando su autenticidad y permitiendo un seguimiento claro de la responsabilidad del médico emisor. Este proceso cumple con las regulaciones legales y mejora la trazabilidad de las decisiones médicas.





Blockchain Federal Argentina en el Sistema Hospitalario:

Blockchain es una tecnología diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible.

La Blockchain Federal Argentina (BFA) es una tecnología de registro distribuido que utiliza una red de nodos para consensuar y validar transacciones. Cada bloque de información está enlazado criptográficamente al anterior, formando una cadena inmutable. La descentralización y la inmutabilidad de la blockchain la hacen adecuada para garantizar la transparencia y la integridad de los registros.
En ese esquema, si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento.

Por su naturaleza, blockchain permite realizar una serie de operaciones combinadas que por primera vez se pueden utilizar de manera conjunta en el mundo digital.

Poder garantizar en cada transacción la identidad de las partes involucradas, ya que todas las transacciones son firmadas criptográficamente.

Certificación de la fecha y hora de la transacción.

La información es inmutable e inalterable: no es posible modificarla ni borrarla.

Toda la información almacenada en la cadena es completamente auditable: se incorpora de forma pública y visible para todos los usuarios.

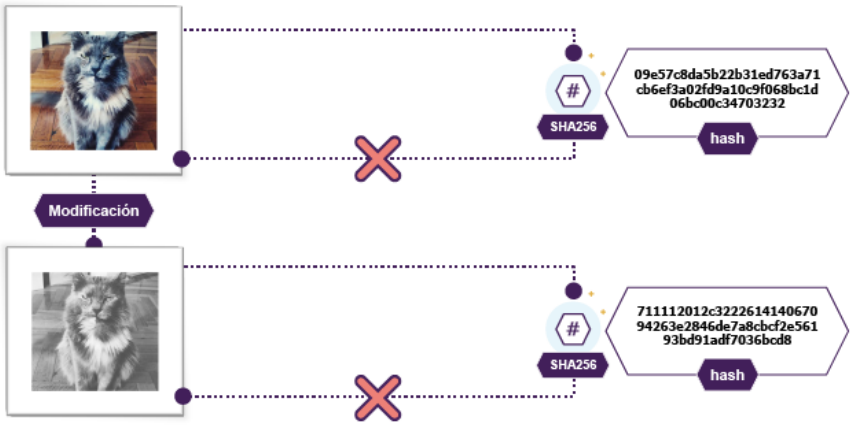
Blockchain funciona sin intermediarios: no hace falta una persona, empresa o institución que legitime la información guardada en la cadena, ya que es segura por naturaleza.

De la misma forma que en un libro contable, las entradas no se pueden borrar o modificar, solo agregar. Una blockchain siempre suma nueva información, crece permanentemente.

Criptografía

Gran parte de la seguridad de la información en Blockchain se debe al uso de métodos criptográficos para encriptarla, y una de las principales herramientas para hacerlo son los llamados hash, o digestos criptográficos.
Un **hash** es un código que se obtiene al procesar información a través de una función. Si modificamos aunque sea algo muy pequeño de esa información, como el color de una foto, o simplemente agregar un acento en un documento de texto, el hash va a cambiar completamente. Los hash suelen llamarse digestos o resúmenes, porque normalmente tienen un tamaño fijo y de pocos dígitos, por ejemplo 64 caracteres en SHA-256.

Esto permite que se garantice la información, ya que al registrar hashes de documentos, podemos tener la certeza de darnos cuenta si alguien cambia su contenido, ya que esas modificaciones harían que el hash de la nueva versión sea completamente diferente.
Esta técnica nos permite dejar de lado la necesidad de almacenar, por ejemplo, fotos en Blockchain. Con solo almacenar el hash, y dejar esa foto en nuestra computadora, servidor o nube, tenemos la certeza de que vamos a darnos cuenta si alguien la modifica. O mejor aún, le estamos ofreciendo al público la certeza de que nosotros, responsables de esa foto, o la podremos modificar sin que nadie se entere.



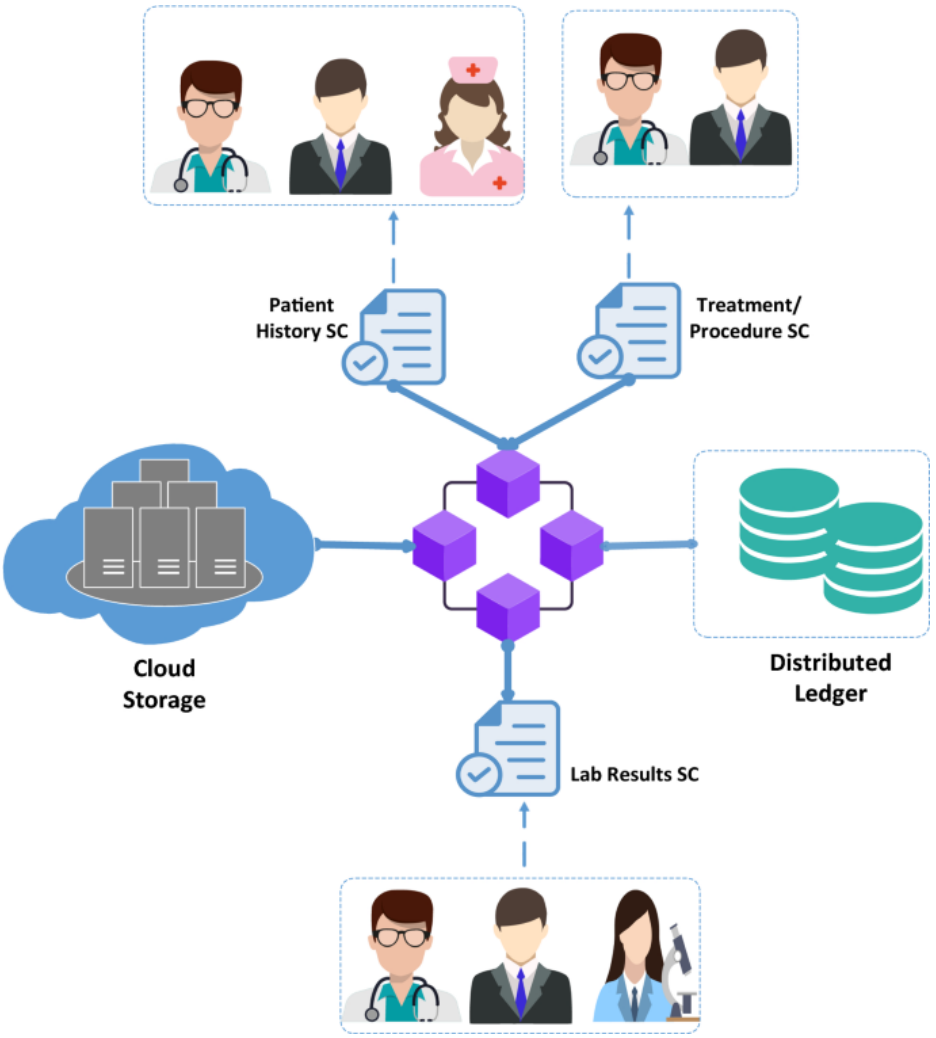
Si hay un mínimo cambio en la foto (como pasarla a blanco y negro) el hash cambia completamente

Al mismo tiempo, como no se puede reconstruir la información original a partir de un hash, nos aseguramos que no le estamos brindando acceso a alguna persona no deseada, por más que ese hash esté registrado públicamente en la blockchain.

Caso de uso específico:

- **Registro de Acceso a Historias Clínicas:**

La blockchain se utilizará para registrar cada acceso a las historias clínicas de los pacientes. Cada vez que un profesional de la salud o personal autorizado acceda a una historia clínica, se generará un registro inmutable en la blockchain. Este enfoque garantiza la transparencia y permite una auditoría completa de los registros de acceso, mejorando la confianza y la seguridad en la gestión de información médica sensible.



Beneficios y Consideraciones:

- **Seguridad Mejorada:** La blockchain y la firma digital fortalecerán la seguridad de la información médica al prevenir accesos no autorizados y garantizar la autenticidad de los documentos.
- **Cumplimiento Normativo:** La implementación cumple con las regulaciones legales relacionadas con la gestión y seguridad de datos médicos.
- **Eficiencia Operativa:** La tecnología contribuirá a una gestión más eficiente de registros y documentos, reduciendo el riesgo de errores y pérdida de información.

Conclusiones:

La integración de la Blockchain Federal Argentina y la firma digital en el sistema hospitalario de John Doe S.A. Proporciona una solución innovadora para abordar los desafíos actuales en la gestión de datos médicos. Estas tecnologías no solo mejoran la seguridad y la transparencia, sino que también cumplen con los estándares legales vigentes.

Referencias:

https://www.argentina.gob.ar/sites/default/files/manual_de_firma_digital_2020.pdf
https://www.utn.edu.ar/es/secretaria-tic/servicios/tic-servicios/firma-digital
https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital
Blockchain - Blockchain Federal Argentina (bfa.ar)
Criptografía - Blockchain Federal Argentina (bfa.ar)