Sistema de Sellado Temporal y Verificación Criptográfica de Documentos

Tecnología Usada: SHA-256 · OpenTimestamps · Blockchain Bitcoin

Autor: Ing. Benjamín Abraham

Fecha: 13/12/2025

1. Introducción técnica

La presente aplicación implementa un **sistema de certificación de existencia, integridad e inmutabilidad de documentos digitales**, basado en **técnicas criptográficas estándar** y en el uso de **registros distribuidos inalterables (blockchain)**.

El objetivo principal del sistema es generar **evidencia técnica verificable**, independiente de la plataforma, del operador y del proveedor, que permita demostrar que un determinado archivo digital **existía en un momento temporal determinado y no fue modificado con posterioridad**.

El sistema se apoya exclusivamente en **estándares abiertos, públicos y auditables**, evitando soluciones propietarias, cerradas o dependientes de terceros de confianza.

2. Principios criptográficos fundamentales

2.1 Funciones hash criptográficas

El sistema utiliza el algoritmo **SHA-256 (Secure Hash Algorithm 256 bits)**, perteneciente a la familia SHA-2 y estandarizado por el **NIST (FIPS PUB 180-4)**.

Una función hash criptográfica presenta las siguientes propiedades relevantes:

- **Determinismo**: el mismo archivo produce siempre el mismo hash.
- **Unidireccionalidad**: no es posible reconstruir el archivo original a partir del hash.
- **Resistencia a colisiones**: es computacionalmente inviable que dos archivos distintos generen el mismo hash.
- **Sensibilidad al cambio**: una mínima modificación del archivo produce un hash completamente diferente.

Estas propiedades convierten al hash en una **huella digital única del contenido**.

2.2 Hash como representación del documento

En este sistema:

- El **hash sustituye técnicamente al documento**.
- El documento **no se almacena, no se transmite ni se registra**.
- Toda la certificación se realiza exclusivamente sobre su huella criptográfica.

Esto permite certificar documentos sensibles sin exponer su contenido.

3. Sellado temporal descentralizado (Timestamping)

3.1 Limitaciones del timestamp tradicional

Los sellados de tiempo tradicionales dependen de:

- Autoridades centrales.
- Servidores de confianza.
- Registros internos modificables.
- Certificados revocables.

Esto introduce riesgos de:

- Alteración ex post.
- Falta de neutralidad.
- Dependencia institucional.

3.2 OpenTimestamps (OTS)

La aplicación utiliza el protocolo **OpenTimestamps**, un estándar abierto para sellado temporal descentralizado.

Características principales:

- No requiere confianza en un tercero.
- No almacena documentos.
- Funciona sobre pruebas criptográficas encadenadas.
- Es verificable públicamente.

3.3 Anclaje en blockchain Bitcoin

El proceso de sellado culmina con el **anclaje criptográfico del hash en la blockchain de Bitcoin**, aprovechando:

- Inmutabilidad del registro.
- Distribución global.
- Seguridad basada en prueba de trabajo (PoW).
- Historial público verificable.

Una vez anclado, el registro:

- **No puede ser alterado sin reescribir la blockchain**.
- Es independiente de la existencia futura de esta aplicación.
- Puede verificarse incluso décadas después.

4. Flujo técnico detallado

4.1 Proceso de sellado

1. Selección del archivo original.
2. Cálculo local del hash SHA-256.
3. Generación de una prueba OTS asociada al hash.
4. Envío del hash al protocolo OpenTimestamps.
5. Agrupación con otros hashes.

6. Anclaje en una transacción de Bitcoin.
7. Emisión del archivo de prueba `.ots`.

4.2 Archivo .ots

El archivo `.ots` contiene:

- La estructura de pruebas criptográficas.
- Los enlaces a la blockchain.
- La información necesaria para verificar el sellado.

No contiene:

- El documento.
- El hash en texto plano (en forma legible).
- Información personal.

5. Proceso de verificación técnica

La verificación puede realizarse en cualquier momento posterior:

1. Se carga el archivo original o su hash.
2. Se carga el archivo `.ots`.
3. El sistema recalcula el hash SHA-256.
4. Se valida la cadena de pruebas OTS.
5. Se verifica el anclaje en la blockchain.
6. Se determina:
    - Coincidencia o no del contenido.
    - Existencia del documento al momento del anclaje.
    - Integridad posterior.

El resultado es **objetivo, reproducible y auditable**.

6. Alcance probatorio

6.1 Lo que acredita técnicamente

- Existencia del documento en una fecha cierta.
- Integridad del contenido.
- Inalterabilidad posterior.
- Trazabilidad criptográfica pública.

6.2 Lo que no acredita

- Autoría.
- Identidad.

- Voluntad.
- Firma manuscrita o digital.
- Legalidad del contenido.

El sistema **no reemplaza** la firma digital ni la certificación notarial, sino que **las complementa**.

7. Valoración jurídica

Desde el punto de vista probatorio, el sistema puede funcionar como:

- Prueba técnica autónoma.
- Medio de corroboración pericial.
- Indicio fuerte de preexistencia documental.
- Soporte para pericias informáticas judiciales.

Su valoración queda sujeta a:

- Normativa aplicable.
- Sana crítica racional.
- Pericia técnica.

8. Seguridad, privacidad y cumplimiento

- No se almacenan documentos.
- No se crean copias.
- No se transmiten contenidos.
- No se procesan datos personales.
- El sistema minimiza riesgos de exposición.

El modelo es compatible con principios de **protección de datos** y **confidencialidad profesional**.

9. Independencia tecnológica

Una vez emitido el `.ots`:

- No depende de esta plataforma.
- Puede verificarse con herramientas abiertas.
- No requiere licencias ni proveedores.

Esto garantiza **perdurabilidad probatoria**.

10. Casos de uso avanzados

- Evidencia digital judicial.
- Prevención de fraude documental.
- Prueba de preexistencia creativa.
- Informes periciales.
- Custodia técnica de documentos sensibles.

- Respaldo previo a litigios complejos.

11. Limitaciones técnicas conocidas

- La fecha es aproximada (ventana de anclaje).
- Requiere acceso a la blockchain para verificación completa.
- No prueba intencionalidad ni contexto.

12. Conclusión técnica

El sistema implementa un **mecanismo robusto, descentralizado y verificable** de sellado temporal de documentos digitales, alineado con las mejores prácticas criptográficas actuales y apto para entornos jurídicos, técnicos y periciales.