27

RMCP

REVISTA MEXICANA DE CIENCIAS PENALES

Psicopatía: biología y cultura

FGR
FISCALÍA GENERAL DE LA REPÚBLICA
INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

Blockchain como estrategia para la prevención del delito de derechos de autor en artesanías textiles: el caso de la biopiratería cultural

Blockchain as a Strategy for Preventing Copyright Infringement in Textile Crafts: The Case of Cultural Biopiracy

Rafael Lara Martínez

Licenciado en Derecho por parte de la Universidad Euroamericana, maestro en Derecho Penal y Criminología por el Centro de Ciencias Jurídicas, y doctor en Derecho del Centro de Ciencias Jurídicas. Es catedrático de la Benemérita Universidad Autónoma de Puebla y del Instituto Tecnológico Nacional en Tehuacán, Puebla.
Correo electrónico: siael@yahoo.com.mx
ORCID: https://orcid.org/0000-0002-9499-9286

Blockchain como estrategia para la prevención del delito de derechos de autor en artesanías textiles: el caso de la biopiratería cultural

Blockchain as a Strategy for Preventing Copyright Infringement in Textile Crafts: The Case of Cultural Biopiracy

Rafael Lara Martínez
Benemérita Universidad Autónoma de Puebla

Recepción: 31/03/2025 **Aceptación:** 26/05/2025

DOI: https://doi.org/10.57042/rmcp.v9i27.912

Resumen

El presente artículo analiza la biopiratería cultural en los diseños textiles indígenas y propone el uso de la tecnología *blockchain* como una política criminal innovadora para su prevención; se expone cómo esta herramienta descentralizada puede certificar la autoría comunitaria mediante NFT, códigos QR o chips NFC, lo que permite la trazabilidad y protección de los conocimientos ancestrales. A través de ejemplos concretos y análisis de costos, se demuestra la viabilidad de registrar estos bienes culturales en redes accesibles como Polygon o Tezos. Por último, se concluye que la *blockchain* puede empoderar jurídicamente a las comunidades y garantizar justicia digital ante el despojo cultural.

Palabras claves:

Blockchain, biopiratería, diseño textil, token, protección.

Abstract

This article analyzes cultural biopiracy of indigenous textile designs and proposes the use of *blockchain* technology as an innovative criminal policy tool for its prevention. It explores how this decentralized tool can certify community authorship through NFT, QR codes, or NFC chips, thereby enabling traceability and protection of ancestral knowledge. Through concrete examples and cost analysis, the article demonstrates the feasibility of registering these cultural assets on accessible networks such as Polygon or Tezos. The study concludes that *blockchain* can legally empower communities and ensure digital justice in the face of cultural appropriation.

Keywords:

Blockchain, biopiracy, textile design, token, protection.

Sumario:

I. Introducción

La biopiratería es un fenómeno que consiste en el apoderamiento indebido de conocimiento ancestral, cuyas titulares son las comunidades indígenas (Gulati, 2019). Dicho acto victimizante lo ejecutan usualmente empresas, aunque también particulares que registran la patente o el derecho de autor. Actual y prácticamente,

todas las comunidades indígenas en Latinoamérica están enfrentando alguna forma de biopiratería por el extractivismo (Valencia-Hernández, Muñoz Villareal y Hainsfurth, 2017), esto es propiciado, en gran medida, porque los registros ante los organismos de propiedad industrial pueden resultar costosos; no es de extrañar que Estados Unidos de América sea el país que obtiene mayores provechos económicos por ser quien puede realizar más registros.

Además, dichos registros deben renovarse cada cierto tiempo, y las disputas legales para dirimir la autenticidad implican uno de los principales problemas de la biopiratería: el determinar quién es el legítimo propietario de un diseño, recurso, inmueble o conocimiento.

Los avances tecnológicos permiten dar autenticidad y veracidad a diversos objetos a bajo costo, con la finalidad de evitar plagio o usurpaciones de cualquier especie. Precisamente la *blockchain* o cadena de bloques puede ofrecer estas bondades. La *blockchain* (o cadena de bloques) es una tecnología que permite registrar información de manera segura, descentralizada y casi inalterable (Linares, Fernández Manzano y González Vasco, 2024). Funciona como un libro del Registro Público de la Propiedad y el Comercio que se distribuye entre muchas computadoras (nodos) en una red; cada vez que se agrega un nuevo registro, se agrupa en un "bloque" que se enlaza criptográficamente con el anterior, de manera que se forma una cadena; propiamente no hay una única entidad que controle la información.

Está distribuida en múltiples computadoras en la red (Llamas Covarrubias, 2021), lo que le atribuye la característica de estar descentralizada, y todos los participantes de la red pueden verificar los registros —aunque en algunos casos, la información puede ser privada—. Cuando un dato se agrega, no se puede modificar sin alterar toda la cade-

na, lo que hace extremadamente difícil el fraude, por ello permite transacciones seguras sin intermediarios, como sí ocurre en el uso de las criptomonedas (García y Rejas, 2022), o con contratos inteligentes, los cuales son programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones, como, por ejemplo, liberar un pago si se verifica la entrega de un producto.

En este sentido, se usa también en el área de la propiedad digital para poder certificar la autenticidad de documentos, títulos de propiedad, patentes o derechos de autor, lo que nos lleva al tema de estudio, pues también puede servir para la protección del conocimiento indígena. Algunas iniciativas buscan registrar el conocimiento ancestral en *blockchain* para evitar la biopiratería y reconocer la autoría de las comunidades.

II. Biopiratería artesanal como hecho victimizante

La Constitución mexicana en su artículo 14 establece el principio de irretroactividad de la ley en perjuicio de persona alguna. Esto significa que no se pueden aplicar leyes penales nuevas a hechos cometidos con anterioridad a su entrada en vigor, si estas leyes resultan más gravosas para el sujeto; por tanto, la falencia radica en que ningún acto de biopiratería artesanal ocurrido antes de la expedición de la Ley Federal para la Protección del Patrimonio Cultural de los Pueblos y Comunidades Indígenas y Afromexicanas, en 2022, puede ser sancionado penalmente con base en esa ley, ya que aún no existía esa tipificación.

Aquí entra el concepto de "hecho victimizante" (Serrano Ceballos, 2023), que no requiere tipificación penal previa, pero sí reconoce la existencia de una afectación concreta a un sujeto o colectivo. Se puede considerar que la biopirate-

ría artesanal es un hecho victimizante cultural y colectivo, especialmente cuando se produce sin consentimiento de la comunidad o bajo engaños, y se lucra con diseños o conocimientos tradicionales sin reconocimiento ni beneficio para los pueblos originarios por descontextualizar el sentido espiritual, ancestral o identitario de una práctica.

Para hablar de "hecho victimizante" se retoma el derecho internacional establecido en los artículos 8 y 15 del Convenio 169 de la Organización Internacional del Trabajo (OIT, 2014), el cual obliga a proteger prácticas culturales y derechos consuetudinarios. También sirve como apoyo la Declaración de la Organización de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas (ONU, 2008), que en sus artículos 11, 12 y 31, establece que los pueblos tienen derecho a la protección jurídica contra el uso no autorizado de sus conocimientos y expresiones culturales, y, por último, el enfoque de la justicia transicional y de los derechos de las víctimas, pues un hecho victimizante no siempre es delito, pero sí puede ser violatorio de derechos humanos y dar pie a mecanismos de reparación simbólica, moral o incluso económica, como parte de una justicia restaurativa o intercultural. Incluso podemos basar el postulado en lineamientos del Sistema Nacional de Atención a Víctimas (CNDH, 2013), donde se considera como hecho victimizante cualquier situación que implique una afectación relevante a los derechos de una persona o colectivo, sin que necesariamente derive en una sentencia penal.

La biopiratería artesanal, aun cuando no era tipificada penalmente en el momento de su comisión, puede ser considerada como un hecho victimizante desde un enfoque de derechos humanos, al implicar una desposesión cultural y simbólica que vulnera los derechos colectivos de los pueblos indígenas, especialmente, su patrimonio inmaterial, identidad y autonomía cultural.

III. Historia del *blockchain*

Se ha llegado a suponer que el origen de las *blockchain* ocurrió en 2008 con la historia de bitcoin (Criado Enguix, 2020), pero en realidad se inicia con las investigaciones sobre criptografía y seguridad informática. Desde sus raíces en los años setenta hasta su uso en criptomonedas y protección de propiedad intelectual, la *blockchain* ha evolucionado de una idea teórica a una tecnología que transforma la economía.

En 1976, Whitfield Diffie y Martin Hellman publicaron el artículo *New Directions in Cryptography* (Diffie y Hellman, 1976), en el que introdujeron el concepto de claves públicas y privadas, que inicia lo que se conoce como criptografía asimétrica. Este modelo es la base de la seguridad en *blockchain*: cada usuario tiene una clave pública (visible) y una privada (secreta). Luego, en 1982, surgió el primer concepto de "cadena de bloques" con David Chaum (Rodríguez Abril, 2020), un pionero en privacidad digital, que propuso un sistema de dinero electrónico seguro basado en criptografía.

Después, en 1991 Stuart Haber y W. Scott Stornetta (Maldonado, 2020) desarrollaron un sistema criptográfico para sellar documentos digitales en el tiempo sin que pudieran alterarse, con lo que por primera vez se usó una "cadena de bloques" con *hashes* criptográficos. En 1998, Nick Szabo (Alvarado Bayo y Supo Calderón, 2021) diseñó un sistema llamado Bit Gold, una forma de dinero digital sin bancos ni intermediarios, que propuso el uso de pruebas criptográficas (prueba de trabajo) para evitar fraudes, un concepto clave en *blockchain*.

En 1997, Adam Back creó Hashcash (Salas Ocampo y Alfaro Salas, 2022), un sistema para evitar *spam* en correos electrónicos que funciona con un mecanismo llamado prueba de trabajo (*proof of work*), que más tarde sería usado en el bitcoin para validar transacciones. Precisamente, el

31 de octubre de 2008, Satoshi Nakamoto (seudónimo de una persona o grupo anónimo) publicó el documento *Bitcoin: A Peer-to-Peer Electronic Cash System* (Zen, 2019), en el que propuso un sistema en el que las transacciones fueran verificadas por una red descentralizada (nodos); este usaba una cadena de bloques para registrar todas las transacciones de forma segura. El 3 de enero de 2009, Satoshi minó el primer bloque de bitcoin, conocido como "bloque génesis" (Marrugo Palomino, 2023), con lo que se creó la primera *blockchain* funcional de la historia.

En 2013, Vitalik Buterin desarrolló Ethereum (Moreno, Garnica Estrada y Sosa, 2024), una *blockchain* mejorada que permitía contratos inteligentes, que pueden ejecutar transacciones sin intermediarios, lo cual abrió el camino para los denominados tokens no fungibles (los NFT, por sus siglas en inglés). Un NFT es un activo criptográfico único (Gámez Baracaldo y Corredor Higuera, 2023) almacenado en una *blockchain*, que usa tecnología de contratos inteligentes para garantizar su autenticidad, propiedad y trazabilidad. Se usa como un folio real digital que actúa como un certificado de autenticidad y titularidad sobre un activo específico, sin posibilidad de alteración o duplicación y cuya inscripción funciona como constancia de autoría o propiedad sobre una obra digital, equiparable a un registro ante una oficina de propiedad intelectual.

En 2014, se creó el primer NFT, conocido como Quantum, creado por el artista digital Kevin McCoy y el programador Anil Dash (Banda, 2022). Se trata de una animación digital en formato GIF que muestra un octágono en movimiento con colores cambiantes. Fue registrado en Namecoin, una de las primeras *blockchains* después de bitcoin, y su propósito era demostrar que se podía vincular una obra digital con un certificado de propiedad único en *blockchain*.

Lo anterior provocó que en 2017 se popularizaran los NFT (tokens no fungibles) que permiten certificar propiedad digital, de manera que surgieron *blockchains* como Tezos, Cardano y Polygon (Koinly, s.f.), que mejoran eficiencia y costos. Actualmente, gobiernos y empresas comienzan a usar *blockchain* para identidad digital, trazabilidad de productos y protección de derechos de autor, además, IBM, Microsoft y la Organización de las Naciones Unidas desarrollan proyectos *blockchain* en logística, salud y justicia.

IV. Funcionamiento de las *blockchain*

Los nodos en *blockchain* son computadoras o dispositivos conectados a la red que almacenan y verifican la información de la cadena de bloques; son los responsables de mantener segura y descentralizada la red. Los nodos están distribuidos en todo el mundo por lo que no hay una ubicación central, ya que la *blockchain* es una red descentralizada y, en consecuencia, cualquier persona o entidad con una computadora y el software adecuado puede operar un nodo y participar en la red.

Existen varios tipos de nodos, pero los principales son los denominados nodos completos (*full nodes*), que guardan una copia completa de toda la cadena de bloques y verifican todas las transacciones (Masumura Ynami y Acosta Chia, 2021); por esto son fundamentales para la seguridad y descentralización de la red, como los que se usan en la red de bitcoin, un nodo completo tiene toda la historia de transacciones desde el bloque génesis.

También existen los nodos ligeros (*light nodes* o SPV *nodes*), que no almacenan toda la cadena de bloques, solo la parte necesaria para validar las transacciones (Garg, 2023), lo que los hace más rápidos y consume menos recursos; un

ejemplo son los utilizados en las aplicaciones móviles de criptomonedas que necesitan verificar pagos sin descargar toda la *blockchain*.

Así también se mencionan a los nodos mineros (*mining nodes* o *criptominers*), que validan y agregan nuevos bloques a la cadena mediante un proceso llamado minería (en redes como bitcoin). Estos necesitan mucho poder de cómputo y energía para resolver problemas matemáticos complejos (Houy, 2016). Los nodos validadores (*staking nodes*) son *blockchains* como Ethereum 2.0 o Cardano; estos, en lugar de minar, validan transacciones a través de un sistema de participación (*staking*), en el que los usuarios bloquean cierta cantidad de criptomonedas como garantía (Haro Olmo, 2024).

Su funcionamiento es el siguiente: cada nodo tiene una copia de la *blockchain* y se comunica con otros nodos en la red, cuando alguien envía una transacción, los nodos verifican que sea válida; si lo es, los nodos la registran en la *blockchain* y la replican en toda la red, esto hace que no haya un solo punto de fallo y que la información sea segura e inmutable. A manera de metáfora, si la *blockchain* fuera un libro del Registro Público de la Propiedad, cada nodo es una persona que tiene una copia idéntica del libro, cuando alguien anota algo nuevo, todos verifican que la anotación es correcta antes de aceptarla, si alguien intenta modificar una página antigua, los demás nodos rechazan el cambio porque no coincide con su copia.

Decía que si imaginamos un libro del Registro Público de la Propiedad donde cada partida es un bloque y está conectada con la partida anterior, cada bloque contiene un conjunto de transacciones (por ejemplo, el registro de un diseño artesanal), un identificador único (*hash*), que es una secuencia alfanumérica generada matemáticamente y el *hash* del

bloque anterior, lo que encadena todos los bloques de forma segura; un ejemplo de una *blockchain* simple sería la que se presenta en la siguiente tabla:

Tabla 1. Ejemplo de *blockchain* simple de registro de un diseño artesanal

```
{
 "bloque": 150982,
 "transacciones": [
  {
   "ID_diseño": "ZX93MNBV09",
   "creador": "Comunidad Zapoteca",
   "fecha": "2025-02-12",
   "hash": "a3f5d9b8e7c4"
  }
 ],
 "hash_bloque_anterior": "8d9c3a4b2e6f"
}
```

Fuente: Elaboración propia.

Aquí, el *hash* del bloque anterior mantiene la integridad de la cadena; si alguien intentara modificar un bloque, todos los siguientes bloques cambiarían, lo que hace casi imposible el fraude. Si una *blockchain* es como un libro del Registro Público de la Propiedad, el legajo sería un NFT, que demuestra a detalle quién es el propietario de lo que está inserto en la partida, al crearse una partida se deja una referencia de la partida anterior que eslabona desde su origen.

Tienen una gran ventaja en su respaldo porque, aunque una computadora que opera como nodo sea destruida, la *blockchain* no desaparece, ya que está descentralizada y distribuida en miles o incluso millones de nodos en todo el mundo. Cada nodo tiene una copia de la *blockchain*, por lo que la pérdida de uno o incluso muchos no afecta a la red en general. Si la computadora o servidor que ejecutaba el

nodo es destruido, simplemente deja de comunicarse con los demás nodos, pero la red *blockchain* sigue funcionando normalmente porque hay muchas otras copias de la cadena en otros nodos, y como está replicada en múltiples nodos, la información sigue intacta en la red.

Cuando un nodo cae, los otros siguen verificando y validando nuevas transacciones y si alguien instala un nuevo nodo con la misma configuración, este se sincroniza con la *blockchain* y vuelve a operar como antes, ya que los nodos nuevos descargan la cadena de bloques desde otros nodos y continúan participando en la red. Esto la hace prácticamente indestructible porque, para que una *blockchain* desaparezca completamente, todos los nodos del mundo tendrían que ser destruidos al mismo tiempo; incluso si una gran cantidad de nodos desaparece, lo peor que pasaría es que la red podría volverse más lenta o vulnerable, pues mientras al menos un nodo quede en pie, la *blockchain* sigue existiendo y otros nodos pueden resurgir, sincronizarse y continuar la cadena.

Un ejemplo de su resiliencia es el bitcoin, que ha sobrevivido ataques y apagones masivos porque su red está distribuida globalmente (Dolader Retamal, Bel Roig y Muñoz Tapia, 2017); si un gobierno prohibiera los nodos en un país, la *blockchain* seguiría existiendo en otros lugares. Incluso se ha propuesto que, para incrementar la fortaleza de la *blockchain*, se almacene en satélites y radios para que no dependa de la infraestructura terrestre.

Una *blockchain* no es meramente una fórmula matemática, usa algoritmos criptográficos para generar los *hashes* que identifican cada bloque. Un ejemplo de una función *hash* SHA-256 (usada en bitcoin y otras *blockchains*), sería que si tomamos el texto "Diseño zapoteca 2025", y aplicamos SHA-256, obtendremos un código único:

"4f8b1d0e91d74cd9bb5b47b5309c34cdb0a74d30e8b9cfb732ac13b9dd92f6c4"

Este código es irrepetible y si se cambia una sola letra en el texto original, el *hash* cambiará completamente. Cada bloque tiene un identificador único (*hash*) que es una secuencia alfanumérica generada matemáticamente, pero la *blockchain* es más que eso, porque se torna como una red descentralizada, en la que muchos nodos verifican las transacciones que usan criptografía para garantizar la seguridad de los datos y permiten crear registros inmutables y rastreables, útiles para proteger diseños textiles.

V. *Blockchain* como mecanismo de prevención del delito de biopiratería artesanal

Las *blockchain* podría ser clave en la protección de diseños textiles y conocimientos ancestrales (Marina, Guarás y Sartor, 2022); se podría registrar la autoría de comunidades indígenas sobre ciertos conocimientos y prevenir la biopiratería, así ha sucedido, por ejemplo, en la India, donde se ha discutido usar *blockchain* para registrar conocimiento tradicional en medicina ayurvédica (Tiwari, 2024) y evitar su explotación por empresas extranjeras.

El método para registrar artesanías en *blockchain* se realizaría mediante el registro por diseño (NFT) para la protección de patrones textiles ancestrales, aunque también puede realizarse un registro por prenda (NFT + QR o NFC) sobre la trazabilidad de cada pieza única. Esto es tangible, puesto que ya existen ejemplos de implementación exitosa de *blockchain* en la protección de bienes culturales inma-

teriales, como IBM Food Trust con la protección de trazabilidad en alimentos (Ravanshree y Devi, 2025); VeChain en moda con el registro de autenticidad de prendas (Davydova, Nahnybida, Adamova, Zhurylo y Tokareva, 2023) y los casos de protección de arte digital mediante NFT (Tezos, Polygon).

Los pasos para vincular un diseño textil con *blockchain* inician con la digitalización del diseño. Se toma una fotografía o escaneo del diseño textil con metadatos clave (nombre de la comunidad, fecha, materiales, técnica utilizada, significado cultural), también se puede usar una marca de agua digital o un patrón oculto para asegurar autenticidad; posteriormente se realiza el registro en *blockchain* y se crea un NFT (token no fungible) del diseño en una *blockchain* como Ethereum, Polygon o Solana.

Este NFT debe contener la imagen del diseño, datos de la comunidad creadora, el registro de autenticidad y las condiciones de uso y derechos de autor; acto seguido, se realiza la asociación con un código QR por medio de la imagen de la prenda y agregándolo a la etiqueta. Al escanearlo con un celular, se puede verificar en la *blockchain* que el diseño es auténtico y pertenece a una comunidad específica. No pasa desapercibido el uso de un chip NFC/RFID en la prenda tejida, pero estamos en el entendido de hacer los costos de forma más accesible para la comunidad indígena.

En términos de costos reales, para registrar un diseño en *blockchain* se debe pagar una tarifa de transacción (llamada *gas fee*), en redes como Ethereum (s.f.). Esta tarifa puede ser alta (de $ 5 a $ 50 USD o más, dependiendo de la congestión de la red), pero otras *blockchain* como Polygon (s.f.), Solana (s.f.) o Tezos (s.f.) son más baratas y pueden costar menos de $ 1 USD por registro. Adicionalmente al costo de creación de un NFT, si se quiere registrar un diseño en

plataformas como OpenSea o Rarible, se paga una comisión inicial; pero algunas plataformas ofrecen *lazy minting*, que permite crear el NFT gratis y pagar solo cuando alguien lo compra. En términos de almacenamiento de datos es barato, pues las *blockchain* no almacenan imágenes directamente, solo guardan el enlace a la imagen alojada en servidores como IPFS (*InterPlanetary File System*), y subir archivos a IPFS (s.f.) es económico, pero si se usa un servicio privado (como AWS o Google Cloud), puede haber costos adicionales. Esto haría que no se protegiera cada prenda individualmente, pero sí, el patrón general.

Tabla 2. Comparación de costos de las *blockchains*

Método	Costo estimado	Dificultad técnica	Beneficios
Blockchain por diseño	$0.10 - $1 USD por diseño	Baja	Protege el patrón general, no requiere equipo extra.
Blockchain por prenda (QR)	Casi gratis (solo impresión de QR)	Baja	Fácil de implementar, ideal para trazabilidad.
Blockchain por prenda (NFC/RFID)	$0.50 - $2 USD por chip	Media	Evita falsificaciones, pero es más costoso.

Fuente: Elaboración propia.

Consideramos que la opción tanto de Polygon como Tezos son las *blockchain* más asequibles, porque permiten registrar información de manera descentralizada y a bajo costo, funcionan principalmente para la creación de NFT (tokens no fungibles), los cuales pueden usarse para

proteger los diseños textiles indígenas; además de que su proceso es relativamente sencillo y se puede hacer a través de plataformas que trabajan con estas *blockchain*, como OpenSea, Objkt o Rarible.

Los pasos son muy básicos para registrar un diseño como NFT en Polygon o Tezos. Primero se debe crear una billetera digital (*wallet*), como MetaMask (para Polygon) o Temple Wallet (para Tezos). Estas billeteras permiten interactuar con la *blockchain* y pagar las tarifas de transacción, luego se carga la imagen del diseño (se recomienda usar IPFS para almacenamiento gratuito) y se añaden datos como el nombre del diseño, descripción y autoría para posteriormente pagar la tarifa de transacción (*gas fee*) —en Polygon, la tarifa puede ser de $ 0.10 a $ 1 USD en Tezos, suele costar entre $ 0.05 y $ 0.50 USD—, y entonces el diseño queda registrado en la *blockchain*. Una vez confirmada la transacción, se genera un enlace donde cualquier persona puede verificar la autenticidad y ya nadie puede modificar ni eliminar el registro.

Hay empresas como Arianee (s.f.), VeChain o Authena que crean chips NFC que enlazan con *blockchain*, estos pueden escanearse con un celular para verificar la autenticidad de la prenda, ya que el chip está vinculado con un NFT en Polygon o Tezos. Cada chip NFC contiene un código único (*hash*) que redirige al NFT en *blockchain*, lo que genera un sistema en el que el usuario escanea la prenda y ve la historia del diseño en *blockchain*.

El costo estimado por chip NFC estándar oscila entre $ 0.50 y $ 2 USD por unidad, mientras que los chips NFC programables con *blockchain* tienen un precio que fluctúa entre $ 2 y $ 5 USD por unidad. En un ejemplo hipotético, si se registra un diseño en *blockchain* usando Polygon y se imprime un código QR en la etiqueta o se inserta un chip NFC,

al escanear el código/chip, el usuario ve los datos del diseño en *blockchain*; si la prenda es revendida, se actualiza la información en *blockchain*.

También se debe considerar el costo de adquisición por chip NFC. Existen diferentes tipos que pueden usarse para vincular una prenda con *blockchain*: para los NFC estándar (etiquetas NFC) serían pequeñas etiquetas adhesivas con un chip programable, se pueden comprar en Amazon, AliExpress o proveedores especializados, su precio ronda entre $ 0.50 a $ 2 USD por unidad.

Asimismo existen los NFC programables con URL personalizada que permite escribir información en el chip y que al escanearlo se abra una página web o *blockchain*; su precio va de $ 1 a $ 5 USD por unidad, y además están los chips NFC de alta seguridad (*blockchain-ready*): empresas como Arianee, VeChain, Authena venden NFC que se integran directamente con *blockchain*, cuyo precio gira entre $ 5 a $ 10 USD por unidad.

Ahora pues, una vez que tenemos los chips NFC, para que apunten a la *blockchain*, necesitamos programarlos con la información del diseño textil en *blockchain*. Un método sencillo es usar OpenSea (Polygon) u Objkt (Tezos) para subir la imagen del diseño y generar un enlace único al NFT en *blockchain*. Después, se procede a programar el chip NFC con esa URL; para ello se utiliza una *app* gratuita como NFC Tools (iOS y Android), para escribir la URL en el chip NFC, y ahora, cada vez que alguien escanee la prenda con un celular, verá el registro en *blockchain*.

Se insiste en que la alternativa más económica es el código QR en lugar de NFC. Si los chips NFC son muy costosos para la comunidad, se puede usar un código QR impreso en la etiqueta.

Tabla 3. Comparación de costos de la NFC y QR

Método	Costo estimado	Ventajas	Limitaciones
NFC estándar	$0.50 - $2 USD	Barato, se puede programar con URL	No tiene alta seguridad
NFC programable con URL	$1 - $5 USD	Se puede enlazar con *blockchain*	Puede ser costoso para grandes volúmenes
NFC *blockchain*-ready (Arianee, VeChain)	$5 - $10 USD	Seguridad máxima, imposible falsificar	Alto costo, requiere proveedor especializado
Código QR impreso	Gratis	Fácil de implementar y usar	Menos seguro que NFC, se puede copiar

Fuente: Elaboración propia.

Debido a que el objetivo es proteger los diseños indígenas de forma barata y accesible, la mejor opción es registrar el diseño en Polygon o Tezos, generar un código QR vinculado al NFT e imprimirlo en etiquetas de tela (costo mínimo), pero si se busca una opción más avanzada, se puede usar NFC programable con un enlace a la *blockchain*.

Ahora bien, en el rubro de los contratos inteligentes para protección legal, se puede programar un *smart contract* en *blockchain* que impida que empresas usen el diseño sin autorización, y si alguien intenta comercializarlo sin permiso, se puede rastrear la transacción. Así también la monetización y reparto de regalías son más sencillos porque si la comunidad permite el uso del diseño, *blockchain* puede automatizar pagos de regalías cada vez que se vende una prenda con ese diseño, es decir, cuando esto ocurra, un porcentaje de la venta se transfiere automáticamente a la comunidad.

Si se quieren programar regalías automáticas para la comunidad en cada venta del diseño, se necesita un contrato inteligente (*smart contract*); cierto es que contratar a un programador para desarrollar un *smart contract* en Solidity (Ethereum) puede costar desde $ 500 USD hasta varios miles de dólares; sin embargo, existen plantillas gratuitas que reducen costos.

Existen casos reales sobre el uso de *blockchain* en textiles, Arianee (Francia) las usa para certificar autenticidad de moda y textiles de lujo, solo que implementa chips NFC en la ropa para vincularla con su registro en *blockchain*. Si se extrapola esta experiencia a los objetivos de esta investigación, se puede tomar un diseño textil ancestral de una comunidad nahua, registrarlo en *blockchain* y crear un NFT con los metadatos del diseño (significado, comunidad creadora, fecha de creación); cuando una marca quiera usar ese diseño, deberá pagar una licencia que queda registrada en *blockchain*.

La opción de *blockchain* por prenda (registro individual de cada pieza textil) funcionaría si cada prenda única recibe un registro, con un número de serie o código QR/NFC individual; esto permitiría que se pueda rastrear quién la compró y si es auténtica, lo cual es útil para evitar falsificaciones y comprobar que la prenda es original de la comunidad. Así, por ejemplo, cada blusa bordada a mano se registra con un NFT único, asociado a un código QR con el que, al escanearlo, el comprador ve la historia del textil, la comunidad que lo creó y su autenticidad. Si alguien revende la prenda, el historial de dueños queda registrado. Lamentablemente, el costo es alto si se registran muchas prendas, puesto que cada una requiere una transacción en *blockchain*.

Siempre puede existir la incógnita de cómo se ve el registro en una *blockchain* con un NFT. En una simulación

para diseño textil, se registraría de la manera que se observa en la tabla 4, y se vería como en la tabla 5:

Tabla 4. Simulación de registro para una *blockchain* con un NFT

Nombre	Diseño Zapoteca #1
Creador	Comunidad Zapoteca
Descripción	Diseño artesanal zapoteca registrado en *blockchain* para proteger su autenticidad y evitar plagio.
Fecha de creación	2025-02-12
Blockchain	Polygon
***Hash* único**	ae2be8c04a61c4f70d067f8bf17a-6261b5aceb621809177c840576a6f-6c56a50
Propietario	0xA1B2C3D4E5F6789
Imagen	https://ipfs.io/ipfs/Qm123xyz
Transacciones	[{'fecha': '2025-02-12', 'accion': 'Creado y registrado en *blockchain*', 'hash_transaccion': '82da140de6d-fefd284610a03cf331a393deffe4c-863810ce48325ad568d89f14'}, {'fecha': '2025-03-01', 'accion': 'Transferido a nuevo propietario', 'nuevo_propietario': '0xB9C8D7E6F5A4321', 'hash_transaccion': '61663d526d82c7e5e064d-625b18082483abf82c08d415241d6e0c-14d3310480c'}]

Fuente: Elaboración propia.

Tabla 5. Simulación de una *blockchain* con un NFT

```
{
"Blockchain": "Polygon",
"Bloque": 157892,
"Fecha de registro": "2025-02-12T14:35:00Z",
"Propietario": "0xA1B2C3D4E5F6789",
"Contrato inteligente": "0x123456789ABCDEF",
"Hash de transacción": "6fcd1653f4e76f828a1603b8a-
6102667407f82faee35419b...",
"Metadata": {
  "Nombre": "Diseño zapoteca #001",
  "Creador": "Comunidad zapoteca",
  "Descripción": "Diseño artesanal zapoteca registrado en blockchain",
  "Imagen": "https://ipfs.io/ipfs/Qm123xyz",
  "Reglas de contrato": {
      "Regalías": "10% al creador en cada reventa",
      "Uso autorizado": "Solo para fines culturales y educativos"
  }
 },
 "Historial de transacciones": [
  {"Fecha": "2025-02-12",
   "Acción": "Creado y registrado en blockchain",
   "Hash de Transacción": "abcd123..."
  },
  {
   "Fecha": "2025-03-01",
   "Acción": "Transferido a nuevo propietario",
   "Nuevo Propietario": "0xB9C8D7E6F5A4321",
   "Hash de Transacción": "efgh456..."
  }
 ]
}
```

Fuente: Elaboración propia.

VI. Conclusiones

Esencialmente las *blockchain* son un sistema descentralizado y seguro para registrar información. Se usan para certificar propiedad digital (como NFT) o para registrar contratos inteligentes.

Así como McCoy protegió Quantum en *blockchain*, los diseños textiles indígenas pueden registrarse como NFT para prevenir plagios y biopiratería, ya que las *blockchain* no son solo para criptomonedas, sino que pueden ser una herramienta de justicia digital ancestral para comunidades indígenas. Así, implementar modelos asequibles permitiría a las comunidades proteger su propiedad intelectual sin depender de sistemas jurídicos costosos; para ello pueden usar códigos QR, que son la opción más barata, y las comunidades podrían autogestionarlos sin necesidad de programadores.

De esta manera, se alcanzarían múltiples beneficios como autenticidad y protección, porque cada diseño ancestral tendría un registro digital inmutable que probaría su origen. También esta propuesta permite la prevención del plagio, porque ni las empresas ni ninguna otra persona podrían usar el diseño sin permiso, ya que su origen es rastreable en *blockchain*. Además, considero que permite un empoderamiento económico, puesto que se crean modelos de licenciamiento que aseguran beneficios económicos para las comunidades.

Cierto es que no se puede "incrustar" literalmente la *blockchain* en un tejido, pero sí se puede asociar un diseño textil con una *blockchain* a través de NFT, códigos QR o chips NFC, lo que permitiría su protección y trazabilidad. Esto podría ser una solución tecnológica contra la biopiratería cultural. Como todo, hay costos al asociar un diseño a una *blockchain*, pero se pueden reducir usando redes más baratas y plataformas que permitan *minting* gratuito, y si el objetivo es proteger diseños indígenas contra la biopiratería, se puede explorar un financiamiento o apoyo institucional.

No obstante, se requiere una legislación sensible a la cosmovisión indígena y el fortalecimiento de capacidades

tecnológicas en las comunidades, para que esta herramienta no reproduzca nuevas formas de exclusión.

VII. Referencias

Alvarado Bayo, María del Carmen Bayo y Daniela Supo Calderón (2021). "*Blockchain* y propiedad intelectual: aplicando una tecnología innovadora en la gestión de Derechos Intangibles". *Themis Revista de Derecho*, *79*, pp. 345-357. https://revistas.pucp.edu.pe/index.php/themis/article/view/24882

Arianee (s.f.). "Soluciones empresariales para pasaportes digitales de productos". *Arianne*. https://www.arianee.com/ [recuperado el 31 de marzo de 2025].

Banda, Aaira (2022). "Non-Fungible Token and Its Applications in the Domain of Fashion, Design and Art". *International Journal of Advanced Research*, *10* (8), pp. 1132–1137. http://dx.doi.org/10.21474/IJAR01/15279

CNDH: Comisión Nacional de los Derechos Humanos (2013). *Lineamientos para la atención integral a víctimas* (3.ª ed.). Ciudad de México: CNDH. https://appweb.cndh.org.mx/biblioteca/archivos/pdfs/Lineamientos-Atencion-Victimas-3-ed.pdf

Criado Enguix, Jaime (2020). "*Blockchain*: criptomonedas y tokenización de activos inmobiliarios. Efectos en el ámbito registral". *Revista de Derecho, Empresa y Sociedad* (*REDS*), *16*, pp. 253–277. https://dialnet.unirioja.es/descarga/articulo/7631171.pdf

Davydova, Iryna, Volodymyr Nahnybida, Olena Adamova, Serhii Zhurylo y Vira Tokareva (2023). "*Blockchain* y procesos civiles: puntos de convergencia". *Revista DIXI*, *25*(1), pp. 1–20. https://doi.org/10.16925/2357-5891.2023.01.01

Diffie, Withfield y Martin Hellman (1976). "New Directions in Cryptography". *IEEE Transactions on Information Theory*, *22*(6), pp. 644–654. https://doi.org/10.1109/TIT.1976.105563

Dolader Retamal, Carlos, Joan Bel Roig y José Luis Muñoz Tapia (2017). "La *blockchain*: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas". *Economía Industrial*, *405*, pp. 33–44. https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf

Ethereum. (s.f.). "La plataforma líder para aplicaciones innovadoras y redes *blockchain*". *Ethereum*. https://ethereum.org/es/ [recuperado el 31 de marzo de 2025].

Gámez Baracaldo, María Camila y Jorge Armando Corredor Higuera (2023). "NFT (token no fungibles) y sus implicaciones en el mercado de valores". *Derecho PUCP*, *90*, pp. 523–564. https://doi.org/10.18800/derechopucp.202301.015

García-Ramos Lucero Miguel Ángel y Ricardo Rejas Muslera (2022). "Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón". *Revista de Internet, Derecho y Política*, *35*. https://dialnet.unirioja.es/descarga/articulo/8399206.pdf

Garg, Rishabh (2023). "*Blockchain* Ecosystem". *Medium*. https://medium.com/@rishabhgargdps/*blockchain*-ecosystem-4fb4e78b30f7 [recuperado el 31 de marzo de 2025].

Gulati, Riya (2019). "Biopiracy, a Biological Theft?". *International Journal of Legal Studies*, *5*(1), pp. 317-350. https://ijols.com/resources/html/article/details?id=190925&language=en

Haro Olmo, Francisco José de (2024). "Ataque del 51 % en *blockchain*: Golpe a la democracia digital". *Scientia Omnibus*

Portus, *4*(7), pp. 1-6. https://dialnet.unirioja.es/descarga/articulo/9562926.pdf

Houy, Nicolas (2016). "The Bitcoin Mining Game". *Ledger*, *1*, pp. 53–68. https://doi.org/10.5195/ledger.2016.13

IPFS (s.f.). "Un sistema abierto para gestionar datos sin un servidor central". IPFS. https://ipfs.tech/ [recuperado el 31 de marzo de 2025].

Koinly (s.f.). "Top 10 Best Crypto Coins to Stake in 2025". *Koinly*. https://koinly.io/blog/best-crypto-to-stake/ [recuperado el 31 de marzo de 2025].

Linares, Rafael, Eva Fernández Manzano y María I. González Vasco (2024). "Oportunidades de la tecnología *blockchain*. La industria cinematográfica: Criptomonedas, tokens y NFTs". *InMediaciones de la Comunicación*, *19*(1), pp. 137–159. https://doi.org/10.18861/ic.2024.19.1.3457

Llamas Covarrubias, Jersain Zadamig (2021). "Transparencia y protección de datos personales en la cadena de bloques (*Blockchain*)". *Estudios en Derecho a la Información*, *11*, pp. 27–63. https://doi.org/10.22201/iij.25940082e.2021.11.15299

Maldonado, Jorge (2020). "¿Quién es W. Scott Stornetta?". *Bit2Me Academy*. https://academy.bit2me.com/quien-es-w-scott-stornetta/ [recuperado el 31 de marzo de 2025].

Marina, Adriana, María Cecilia Guarás y Paulo Sartor (2022). "Habitus y apertura tecnológica mediante la inclusión de *blockchain* en las comunidades originarias de artesanos de los Andes". *Cuadernos del Centro de Estudios en Diseño y Comunicación. Ensayos*, *111*, pp. 207–220. https://dx.doi.org/10.18682/cdc.vi111.4241

Marrugo Palomino, Oscar D. (2023). "Análisis de los elementos que generan confianza en el dinero y las criptomonedas".

Revista Colombiana de Contabilidad - ASFACOP, *11*(22). https://ojs.asfacop.org.co/index.php/asfacop/article/view/289

Masumura Ynami, Dana Lorena y Valeria Alejandra Acosta Chia (2021). "Atando los nodos sueltos: *Blockchain* para la reducción de corrupción en las licitaciones públicas de ProInversión". *THĒMIS-Revista de Derecho*, *79*, pp. 141–153. https://doi.org/10.18800/themis.202101.008

Moreno, Ernesto Ilich, Evelyn Garnica Estrada y José Vicente Sosa (2024). "Contratos digitales usando Ethereum: Una revolución en la contabilidad". *Revista Colombiana de Contabilidad*, *12*(24), pp. 99-120. https://dialnet.unirioja.es/descarga/articulo/10041247.pdf

ONU: Organización de las Naciones Unidas (2008). Declaración de las Naciones Unidas sobre los derechos de los pueblos indígenas. ONU. https://www.un.org/esa/socdev/unpfii/documents/DRIPS_es.pdf

OIT: Organización Internacional del Trabajo (2014). Convenio núm. 169 de la OIT sobre pueblos indígenas y tribales. Declaración de las Naciones Unidas sobre los derechos de los pueblos indígenas. Perú: OIT. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@americas/@ro-lima/documents/publication/wcms_345065.pdf

Polygon (s.f.). *Web3, Aggregated*. https://polygon.technology/ [recuperado el 31 de marzo de 2025].

Ravanshree, M. y M. Devi (2025). "IBM Food Trust: Revolutionizing the Food Supply Chain with *Blockchain*". *Agri Articles*, *5*(1), pp. 292–295. https://agriarticles.com/wp-content/uploads/2025/01/E-05-01-91-292-295.pdf

Rodríguez Abril, Rubén (2020). "¿Puede la tecnología DLT servir de base para la creación de un nuevo ordenamiento cambiario electrónico?". *Internacional de Derecho de la Comuni-*

cación y de las Nuevas Tecnologías, *29*, pp. 75–103. https://revistas.ucm.es/index.php/DERE/article/view/90889

Salas Ocampo, Luis Diego y Marly Alfaro Salas (2022). "Criptomonedas y su efecto en la estabilidad del sistema financiero internacional: Apuntes para Centroamérica". *Revista Relaciones Internacionales*, *95*(1), pp. 33-77. https://dialnet.unirioja.es/descarga/articulo/8886562.pdf

Serrano Ceballos, Jorge (2023). "La atención a víctimas centrada en la persona". *Revista Mexicana de Ciencias Penales*, *6*(19), pp. 99–122. https://doi.org/10.57042/rmcp.v6i19.607

Solana (s.f.). "Infraestructura Web3 para todos". *Solana*. https://solana.com/es [recuperado el 31 de marzo de 2025].

Tezos (s.f.). "Una plataforma *blockchain* de código abierto para activos y aplicaciones". *Tezos*. https://tezos.com/ [recuperado el 31 de marzo de 2025].

Tiwari, Shruti (2024). "Ayurvastra: La confluencia de la medicina tradicional y la moda sostenible". *International Journal for Multidisciplinary Research*, *6*(1), pp. 1–10. https://doi.org/10.36948/ijfmr.2024.v06i01.10363

Valencia-Hernández, Javier, Erika Muñoz-Villarreal y Jenny-Carolina Hainsfurth (2017). "El extractivismo minero a gran escala: Una amenaza neocolonial frente a la pervivencia del pueblo Embera". *Revista Luna Azul*, *45*, pp. 419–445. https://www.redalyc.org/journal/3217/321753629021/

Zen, Daniel (2019). "La dimensión semiótica en el modelo transaccional de Bitcoin". *deSignis*, *30*, pp. 209–215. https://doi.org/10.35659/designis.i30p209-215

DOSSIER

VARIA

RESEÑA

Revista Mexicana de Ciencias Penales
Número 27 / Publicación cuatrimestral
septiembre-diciembre 2025 / Año 9 / Segunda época
ISSN: 0187-0416 / e-ISSN: 2954-4963
$200.00 MXN

Versión OJS
revistacienciasinacipe.fgr.org.mx

FGR FISCALÍA GENERAL DE LA REPÚBLICA

INACIPE INSTITUTO NACIONAL DE CIENCIAS PENALES

INACIPE 49 AÑOS 1976 • 2025