Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo final

Título

Cadena de bloques: potencial aplicación a Historias Clínicas Electrónicas

Autor: Ing. Joffre Aguirre

Director de Tesis: Dr. Pedro Hecht

Año 2017

Cohorte 2016

Declaración Jurada:

"Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual"

FIRMADO

Joffre Armando Aguirre Regato

DNI: 95.564.253

PASAPORTE: 091835743

Tabla de contenidos

Introducción

El presente trabajo explica en detalle la cadena de bloques desde su nacimiento como Bitcoin hasta su establecimiento como una tecnología emergente y expone su aplicación en el campo de la salud. Bitcoin fue la primera cadena de bloques con propósito financiero para crear una criptomoneda, en el trabajo se explica desde el minado sobre el bloque Génesis realizado por Satoshi Nakamoto el 3 de enero del 2009 hasta el último *hard fork* realizado en la red el 31 de julio del 2017.

Bitcoin nace como un conjunto de algoritmos que integró Nakamoto para poder definir un modelo de moneda criptográfica usando: firmas digitales, el modelo de B-money, servidor de marcas de tiempo estilo Usenet basándose en una evolución del modelo de Hashcash. Así mismo, contribuyó con ideas propias como las reglas de consenso de la red, el modelo de privacidad y el esquema de incentivos para la minería.

En un análisis de componentes de Bitcoin observaremos como la cadena de bloques es la solución central de la criptomoneda. Bitcoin se compone de las transacciones, la red *Peer to Peer* (P2P), la minería, las reglas de consenso, llaves criptográficas privadas y públicas. Analizando cada una de estas tecnologías se puede llegar a concluir que Bitcoin es solo una aplicación de la cadena de bloques. Bitcoin tiene algunas cosas adicionales como los monederos que son aplicaciones clientes para manejar las llaves criptográficas de los usuarios, pero en su modelo central es una cadena de bloques con la particularidad que retiene la historia de valores desde su creación hasta sus últimos propietarios, además de transportar el valor dentro de cada bloque de tal manera que el dato queda registrado de forma secuencial en el tiempo.

Tenemos que citar las principales características de seguridad como el anonimato, privacidad, trazabilidad y confiabilidad que aporta la cadena de bloques. Hoy en día, con una computadora cuántica desarrollándose para atacar ciertos problemas que consideramos de complejidad en tiempo

Nondeterministic Polynomial Time (NP), debemos citar los avances que se están realizando con la primera cadena de bloques con soporte ante ataques cuánticos usando un esquema de *Quantum Key Distribution* (QKD) entre pares para prevenirlos, donde se perdería la característica de privacidad, pero se ganaría resistencia ante ataques cuánticos [1].

Si bien la cadena de bloques nació como una criptomoneda, se puede aplicar como solución a muchos problemas basados en sus características de anonimato, privacidad, integridad y trazabilidad. Se analizarán los requerimientos exigidos para la manutención de los registros de salud dentro del marco legal de los Estados Unidos de América, revisando las leyes y las iniciativas que plantean las agencias que apoyan el desarrollo de la salud para elegir a la Cadena de Bloques como una solución. Así mismo, revisaremos propuestas de implementaciones que fueron publicadas en el 2016, como respuesta a un desafío lanzado por el gobierno de los Estados Unidos.

Objetivos específicos

Se explicará al detalle la criptomoneda Bitcoin y todos sus componentes, debido a que dio inicio a la tecnología cadena de bloques. Es decir, cadena de bloques no existía como tecnología antes del 2009 donde aparece en el informe de Satoshi Nakamoto [2].

Como segundo paso se profundizará en la cadena de bloques y sus características, además de brindar un estado del arte de la tecnología y los posibles usos que se están planteando en la actualidad.

Para finalizar, se revisará un posible campo de aplicabilidad de la cadena de bloques en el contexto de salud. Se analizará la problemática actual de las historias clínicas electrónicas y los sistemas de gestión hospitalaria. Y se explicarán algunas propuestas de implementación en este campo.

Desarrollo

1. Descripción de Bitcoin

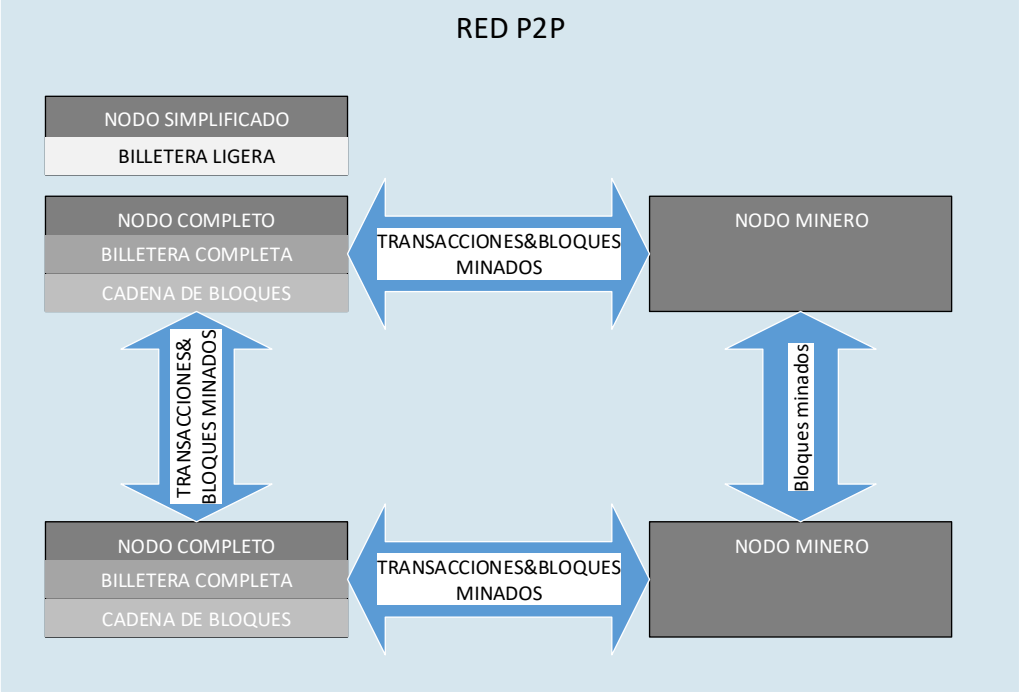
Se comenzó a realizar el diseño de la criptomoneda Bitcoin en el 2008 cuando Nakamoto publicó su informe “Un Sistema de efectivo electrónico

usuario a usuario” [3]. En el 2009 se minó el primer bloque Bitcoin y luego se dio a conocer como el bloque Génesis.

Bitcoin es una moneda criptográfica y funciona en un entorno distribuido. A diferencia del dinero en papel y el “dinero electrónico” se basa en la fortaleza de la criptografía usando firmas digitales para demostrar su autenticidad y propiedad, por lo tanto, no necesita de un ente central de confianza para testificar o dar confianza a la transacción.

Como cita Nakamoto en su informe “Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas, realizar transacciones directamente sin la necesidad de un tercero confiable” [3], Bitcoin logra esta meta a través de su diseño mostrado en la figura inferior al agrupar varios sistemas: Billetera, Transacciones, Protocolo par a par *bitcoin*, Cadena de bloques *Blockchain* y Minería.

Figura 1.1 Componentes de Bitcoin



Fuente: Elaboración propia

En las siguientes secciones se describirán todos estos componentes y tecnologías claves para el funcionamiento de Bitcoin.

1.1 Billetera

Una Billetera o *Wallet Bitcoin* es un repositorio de direcciones privadas y públicas las cuales son propiedad del usuario. Las direcciones privadas son llaves privadas criptográficas que garantizan la propiedad de los Bitcoins y permiten gastar los Bitcoins asociados a sus respectivas direcciones públicas de Bitcoin.

Existen dos tipos de billetera: Aleatoria o no determinista y la Basada en Semilla o Determinista. Para explicar estas billeteras se revisarán los conceptos de direcciones Bitcoin.

1.1.1 Direcciones Bitcoin.

Las direcciones Bitcoin se pueden dividir en privadas y públicas. Se describirá en esta sección cómo se generan las direcciones y cómo se usan.

Direcciones Bitcoin Privadas.

Una dirección privada bitcoin es usada para comprobar su propiedad y gastar los Bitcoins asociados. Generar una dirección privada k es crear un número aleatorio entre 1 y n-1, donde $n=2^{256}-2^{224}+2^{192}+2^{96}-1$ (Curva elíptica de orden 256 y característica 2 sobre un campo finito polinómico basada en el modelo secp256k1). “k” será definido como nuestra llave privada de 256 bits (64 bytes) [4]. Para Bitcoin se adoptan varios formatos resumidos en la siguiente figura:

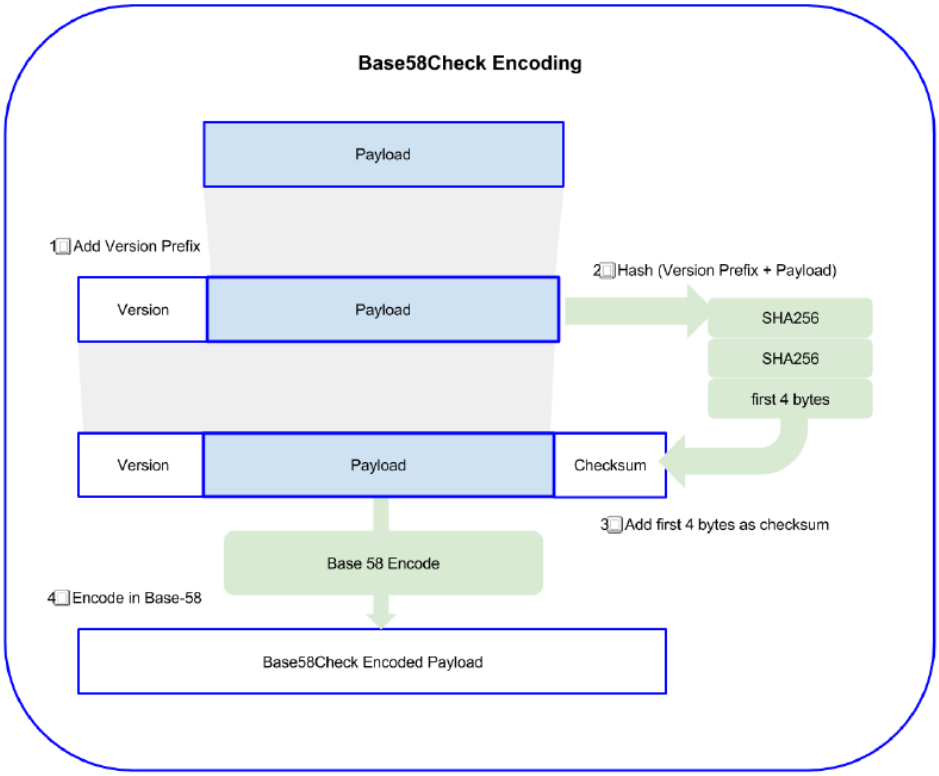
Figura 1.2 Claves privadas en diferentes formatos

Formato	Clave privada
HEX	E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262
WIF	5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF

Fuente: Elaboración propia.

Wallet Import Format (WIF), corresponde a un formato más agradable que hexadecimal y menos propenso a errores humanos, éste utiliza Base58Check [5] como codificación. También adiciona un byte de versión (prefijo de versión 0x80 para claves privadas) y 4 bytes de chequeo de error en la propia dirección basado en un doble hash SHA-256. Para direcciones privadas nótese que se iniciará con el carácter ‘5’. El proceso se observa en la siguiente figura:

Figura 1.3 Codificación Base58Check



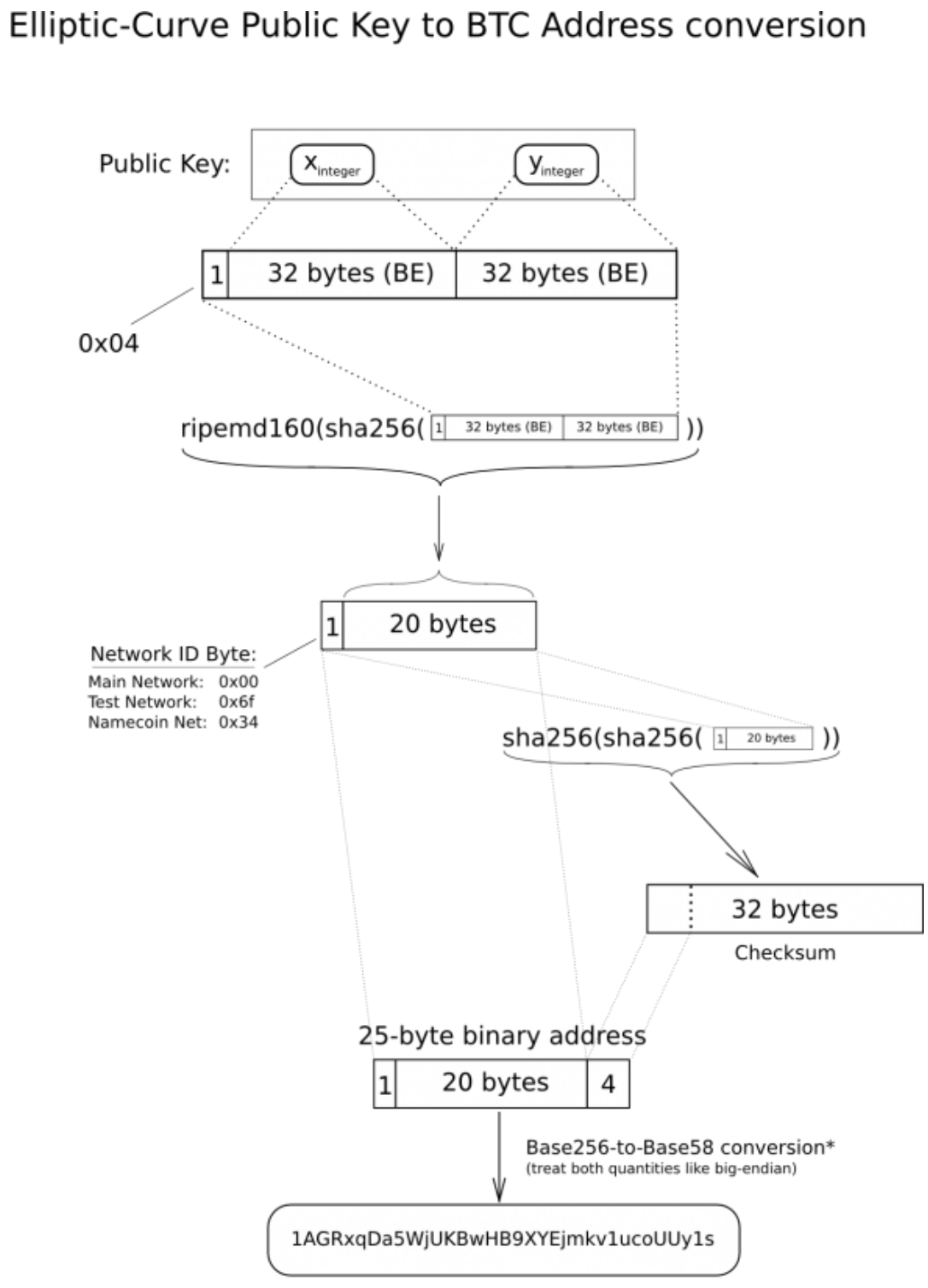
Fuente: [6]

La especificación BIP0032 [7] permite el uso de claves privadas de hasta 512 bits, pero son usadas en carteras deterministas, donde se utiliza la clave privada como semilla y entonces derivar un árbol de claves.

Direcciones Bitcoin publicas

Este tipo de direcciones son generadas a través de la clave privada k y usa la especificación secp256k1. Consiste en seleccionar un punto de la curva elíptica C definida sobre un campo polinómico de Gallois del orden 256 y característica 2. Se usa el punto Generador G definido en secp256k1 para realizar la operación: K=k*G; donde K viene a ser nuestra clave pública. La clave pública K se transformará en una dirección pública Bitcoin al ejecutar un HASH160 = RIPEMD160(SHA256(0x04+K)), se añade el chequeo de errores y al finalizar se codifica Base58Check como se observa a continuación:

Figura 1.4 Codificación Bitcoin de una clave pública



Fuente: [6] [5]

Las direcciones públicas de Bitcoin son cadenas de 20 bytes y pueden tener algunos prefijos como se muestra a continuación:

Figura 1.5 Claves Bitcoin públicas: 0x00, 0x05, 0x0488B21E. Claves privadas 0x80, 0x0142.

Tipo	Prefijo de versión (hexadecimal)	Prefijo del resultado Base58
Dirección Bitcoin	0x00	1
Dirección Pago-a-Hash-de-Script	0x05	3
Dirección de Testnet Bitcoin	0x6F	m o n
WIF de Clave Privada	0x80	5, K o L
Clave Privada con Encriptación BIP38	0x0142	6P
Clave Pública Extendida BIP32	0x0488B21E	xpub

Fuente: [6]

1.1.2 Billetera aleatoria

Este monedero aún se conserva en la Bitcoin Core o cliente de referencia. Fue diseñada con un repositorio de llaves privadas generadas aleatoriamente y direcciones publicas Bitcoin. El respaldo o migración de este tipo de carteras requiere esfuerzo por la cantidad de llaves privadas a portar, ya que cada transacción donde utilicemos una dirección pública requeriría un respaldo. En Bitcoin se puede generar una llave pública por cada nueva transacción a realizar y esto dará como resultado en tantas llaves como transacciones tenga el monedero, aunque bien se puede usar la misma dirección pública Bitcoin para varias transacciones. Sin embargo, no se puede compartir este tipo de billeteras entre varios sistemas simultáneamente debido a la gran cantidad de llaves y memoria requerida.

1.1.3 Billetera determinista

El monedero *hierarchical deterministic* (HD) o billetera determinista se basa en una sola semilla para una clave privada máster, a partir de la cual se generarán todas las demás llaves privadas y públicas. Se produce un ahorro de esfuerzo para el respaldo o migración de este tipo de billeteras. Por su estructura, solo se debe portar la llave semilla y el modelo determinista recreará todo el árbol de claves. El BIP0032 [7] define este tipo de billeteras.

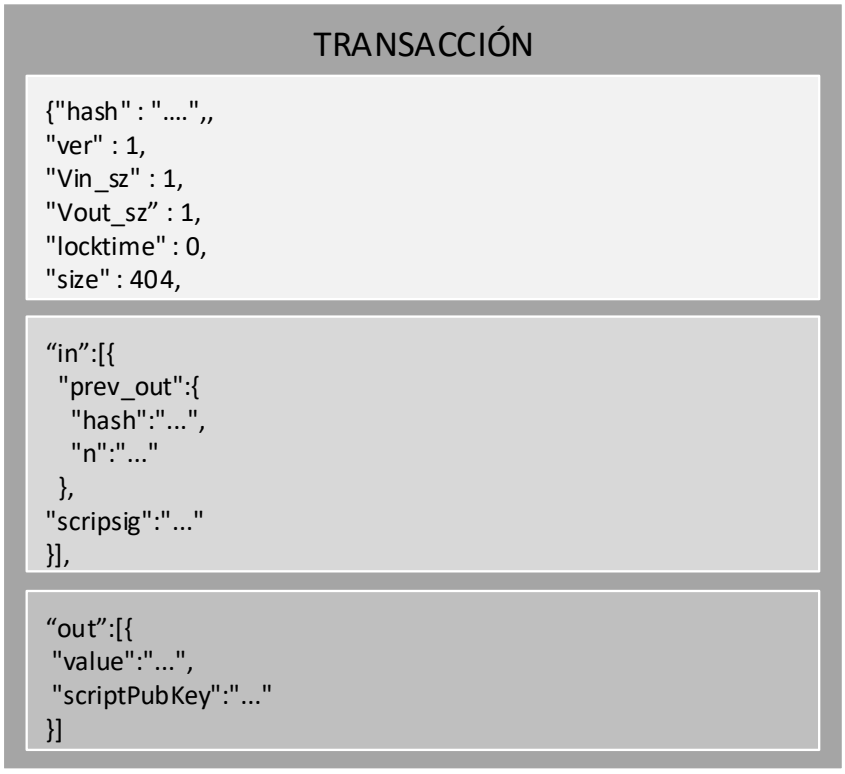
1.2 Transacciones Bitcoin.

“Definimos una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un hash de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para comprobar la cadena de propiedad” [3].

Se define una transacción Bitcoin como una transferencia de valor de un ente a otro, entiéndase por ente a una dirección Bitcoin. Para entender este concepto se debe olvidar el modelo mental basado en cuentas, en otras palabras, no se acredita o debita saldo de una cuenta. El modelo Bitcoin se base en un modelo de libro de contabilidad, donde se transfiere valor de un ente a otro. Esto da como resultado saldos en las salidas de este llamado libro de contabilidad o Cadena de Bloques [8].

Una transacción Bitcoin consta de tres componentes esenciales: Metadata, Inputs y Outputs como se indica en la figura:

Figura 1.6 Componentes de una transacción.



Fuente: Elaboración propia

1.2.1 Metadata

La Metadata contiene los siguientes campos: *Ver*, *Hash*, *Vin_sz*, *Vout_sz*, *Size*, *Lock_time*.

Ver es el campo de 4 bytes de la versión y está definido en 1.0, definido por Satoshi, indica que juego de reglas aplican a la transacción, este campo permite ir evolucionando a las transacciones manteniendo compatibilidad hacía atrás. Hash_id es un campo de 20 bytes y funciona como un ID único que permite usarlo como puntero a la transacción.

vin_sz y *vout_sz* son campos de longitud variable entre 1 a 9 bytes que permiten especificar la cantidad de entradas y salidas de una transacción.

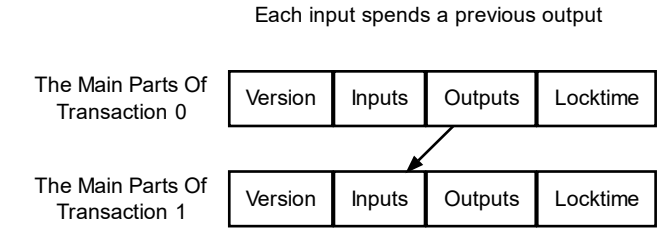
Size es el tamaño en bytes de la transacción.

Lock_time es un campo de 4 bytes y se define como un sello de tiempo unix, el cual permite especificar el tiempo de ejecución de una transacción (una analogía a un instrumento financiero post fechado). Por lo general, está configurado a cero para indicar que la transacción debe ser procesada de inmediato por los nodos. Si el valor es menor a 500 millones se interpreta como una transacción que no debe ser procesada hasta alcanzar la altura especificada en bloques. Si el valor es mayor a 500 millones es interpretado como una marca de tiempo para poder ejecutar la transacción cuando se cumpla el tiempo especificado.

1.2.2 Entradas

Las entradas representan un arreglo de hashes que son punteros a transacciones anteriores. Estos deben ir firmados con nuestra clave privada para que puedan ser gastadas. Cuando se habla de transacciones anteriores se refiere a transacciones donde una dirección pública de Bitcoin asociada a nuestro monedero fue la salida de una transacción, estas son conocidas como transacciones sin gastar *Unspent Transaction Output* (UTXO) como muestra la figura.

Figura 1.7 Ejemplo de Entrada de transacción que apunta a una salida previa.



Fuente: [2]

Se debe notar que las entradas no tienen un campo de valor debido a que se deben gastar en su totalidad en una transacción. En otras palabras, para pagar a una dirección pública de Bitcoin se deben acumular tantas entradas para que la suma sea mayor o igual al valor de salida. En el siguiente grafico se puede apreciar la estructura de una entrada:

Figura 1.8 Estructura de la entrada de una transacción

Tamaño	Campo	Descripción
32 bytes	Hash de Transacción	Puntero a la transacción que contiene la UTXO a ser gastada
4 bytes	Índice de Salida	El número de índice de la UTXO a ser gastada; comenzando por 0
1-9 bytes (VarInt)	Tamaño del Script de Desbloqueo	Longitud del Script de Desbloqueo en bytes, a seguir
Variable	Script de Desbloqueo	Un script que cumple con las condiciones del script de bloqueo de UTXOs
4 bytes	Número de Secuencia	Funcionalidad de reemplazo de transacción actualmente deshabilitada, establecer en 0xFFFFFFFF

Fuente: [8]

1.2.3 Salidas

Las salidas representan un arreglo con dos campos: un valor en Satohis (1BTC = 100000000 Satoshis) y un script de bloqueo de transacción. En la sección tipo de scripts vamos a explicar los scripts de bloqueo. Las salidas tienen una limitante: la suma de los valores de salida siempre debe ser menor o igual a la suma de los valores de las transacciones referenciadas en las entradas. Si la cantidad de entradas es mayor a la salida se debe

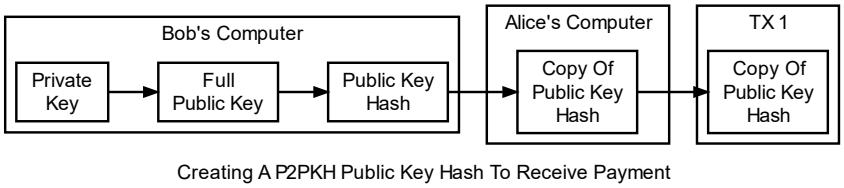
generar un valor de cambio hacia una dirección pública del originador de la transacción. Por consiguiente, cuando no se genera la dirección de salida Bitcoin con la diferencia entre salida y entrada, el minero del bloque asume que ese valor corresponde a la comisión por ingresar la transacción en el bloque a minar.

1.2.4 Tipos de scripts en las salidas de Bitcoin

Las transacciones Bitcoin en las salidas usan varios tipos de scripts, los cuales son *Pay to Public Key Hash* (P2PKH) o Pago a hash de direcciones públicas, Pay to Public Key (P2PK) o Pago a clave pública, MULTISIG o Multifirma, *Pay to Script Hash* (P2SH) o Pago a hash script. Bitcoin usa un lenguaje de script basado en *Forth*, el cual usa una programación especial basado en Pila o *Stack*. Este lenguaje se interpreta de izquierda a derecha, donde los valores se guardan en el *Stack* y mediante comandos específicos se realizan operaciones con los datos. Se debe notar que en los *scripts* se usan direcciones bitcoin en formato hexadecimal sin compresión.

P2PKH es un tipo de *script* simple que indica que los valores son bloqueados para un *hash* de una dirección pública de Bitcoin. Cuando el ente A realiza una transacción y asigna fondos al ente B lo que hace es lo siguiente: B genera una clave privada y en base a esta construye una dirección pública Bitcoin (clave pública con *hashing*). B entrega la dirección pública al ente A, con esta información se construye la transacción TX1 P2PKH como se muestra en la figura.

Figura 1.9 Construcción de una transacción P2PKH



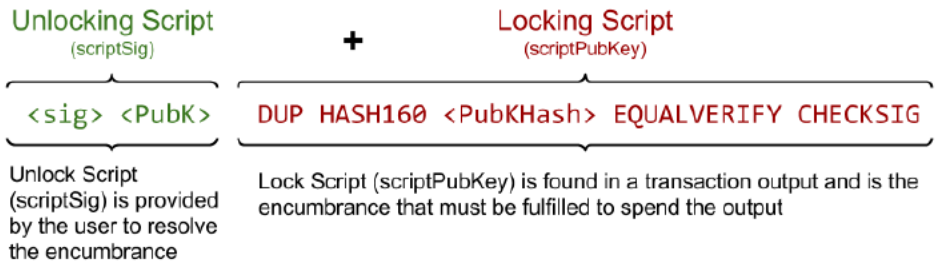
Fuente: [2]

Una vez creada la transacción será validada y propagada por cada nodo de la red. Una vez minada la transacción aparecerá en la billetera de B

como una UTXO con valores disponibles asignados la dirección pública de B, así como en todos los nodos Bitcoin.

B para gastar esos fondos debe probar su propiedad generando un *script* de desbloqueo que es una firma *Elliptic Curve Digital Signature Algorithm* (ECDSA) [4] de su clave pública más su clave pública en claro como se muestra en la figura. Cualquier nodo al verificar la propiedad de la UTXO deberá obtener TRUE como resultado para poder propagar la transacción.

Figura 1.10 Ejemplo de script de desbloqueo y su respectivo script de bloqueo P2PKH.



Fuente: [8]

P2PK es el mismo tipo de script P2PKH, pero con la clave pública sin *hashing*. En consecuencia, el script de bloqueo se vuelve más simple:

<Public Key B> OP_CHECKSIG

La sección de desbloqueo se ve así:

<Sign from Priv Key B>

Dando como resultado el script combinado:

<Sign from Priv Key B> <Public Key B> OP_CHECKSIG

No es recomendable usar este tipo de scripts porque hace crecer el tamaño de la transacción, si considera k de 256 bits, entonces K sería de 512 bits, donde K=kG, siendo G una coordenada de la Curva elíptica. Esto da como resultado un script de bloqueo con una llave pública más larga y transmite un costo de minería al originador de la transacción.

MULTISIG es similar al P2PKH, pero con la opción de poder anotar hasta 15 firmas en un script de bloqueo hasta la versión actual de Bitcoin. En el script presentado abajo se debe notar que M es la cantidad de firmas necesarias de N claves públicas para validar el script.

<M> <PK 1> <PK 2> … <PK N> <N> OP_CHECKMULTISIGN

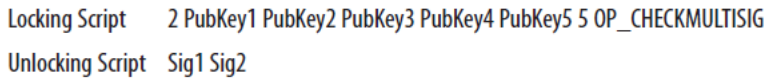
Da como resultado una sección de desbloqueo así:

OP_0 <Sign Priv Key 1> <Sign Priv Key 2> … <Sign Priv Key M>

Se incluye el OP_0 por defecto debido a un error al momento no corregido, pero se pueden construir *scripts* potentes multifirmas. Al igual que P2PK se debe notar el uso de la clave pública sin *hashing*. Estos *scripts* poseen la debilidad de ser muy largos y difíciles de transmitir a los que deseen usarlos.

P2SH es un tipo de *script* potente porque combina la simplicidad de P2PKH y la complejidad de MULTISIG. Para dar un ejemplo se puede revisar un *script* de bloqueo y desbloque multifirma donde se necesitan dos de 5 firmas para poder realizar el desbloqueo como se puede ver en la siguiente figura:

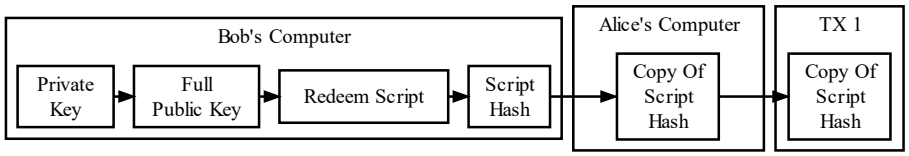
Figura 1.11 Scripts para una multifirma 2 de 5



Fuente: [8]

Analizando el *script* multifirma se requiere pasar al originador de la transacción 5 claves públicas de 512 bits para que pueda crear un *script* de complejidad media. Tomar en cuenta el costo de minado de la transacción que depende del tamaño de la transacción en bytes. En el 2012 Bitcoin tuvo la idea de proporcionar un *hash* de *script* en vez de una dirección pública Bitcoin como se muestra en la siguiente figura:

Figura 1.12 Creando un Hash de script para recibir un pago.



Creating A P2SH Redeem Script Hash To Receive Payment

Fuente: [2]

El *Redeem Script* o script de liquidación será el *script* real que contenga toda la cadena de claves públicas, dando como resultado los siguientes ítems mostrados en la figura:

Figura 1.13 Script multifirma representado en un Hash Script.

Redeem Script	2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 5 OP_CHECKMULTISIG
Locking Script	OP_HASH160 <20-byte hash of redeem script> OP_EQUAL
Unlocking Script	Sig1 Sig2 redeem script

Fuente: [8]

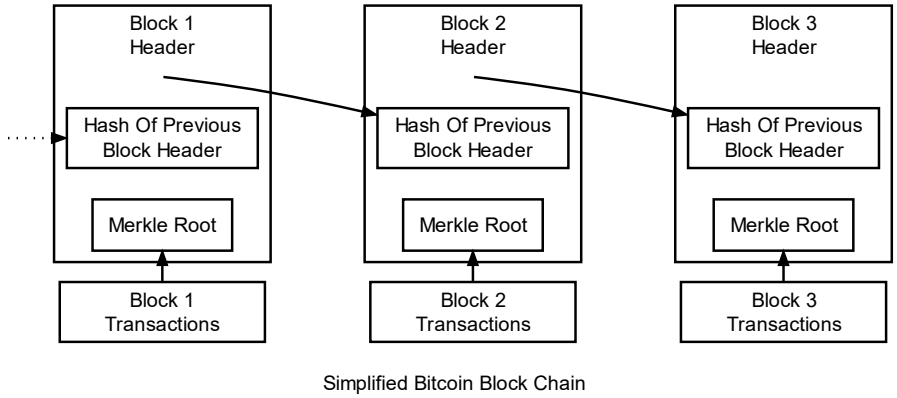
Esto permitirá que entreguemos a A solamente un script de 20 bytes que es una dirección bitcoin especial, la cual inicia con el carácter “3” vista en base58Check.

P2SH es muy potente y el nodo para validar la transacción debe hacerlo en dos etapas, primero ejecuta el hashing del script y comprueba que sea igual antes de pasar a verificar su contenido. La transacción tipo OP_RETURN será discutida en otra sección ya que no es una operación estándar de Bitcoin.

1.3 Cadena de Bloques.

La cadena de bloques (*Blockchain)* provee un libro mayor público de registro de bloques de transacciones Bitcoin ordenadas en forma cronológica. Este sistema es usado para solucionar el problema del doble gasto y prevenir la modificación de transacciones previas [3]. Los bloques están enlazados hacia atrás en el tiempo referenciando a su bloque antecesor tal como se muestra en la figura:

Figura 1.14 Modelo simplificado de la cadena de bloques



Fuente: [2]

El modelo conceptual usado es una pila de bloques donde el más reciente está en la cima, por eso cuando se mencione altura nos referimos al tamaño de la cadena o el número del último bloque. Como se puede ver cada bloque tiene en su cabecera un identificador *hash* SHA256 y el identificador del bloque anterior o padre, de esta forma se encadenan los bloques hasta el bloque Génesis.

Todos los nodos mantienen la cadena de bloques actualizada y para insertar un nuevo bloque deben invertir poder computacional para solucionar un reto de cierta complejidad. Este reto se llama *Proof of Work* (PoW) o prueba de trabajo, todos los nodos honestos trabajan duro para solucionar dicha prueba, lo cual hace difícil estadísticamente modificar un bloque previo. Así mismo, para mantener la misma copia de la cadena de bloques en todos los nodos existen reglas de consenso iguales para todos los nodos. La prueba de trabajo y las reglas de consenso se explicarán en detalle en el capítulo cadena de bloques.

Un bloque puede tener un solo padre, pero más de un hijo. Esta condición se produce debido a que dos mineros en la red bitcoin puede resolver “simultáneamente” un bloque y anunciarlo. La red bitcoin se autocorregirá en el momento que otro minero anuncie un bloque hijo de una de las ramas y el protocolo descarte la rama más pequeña. Esta condición se analizará en detalle en el capítulo dedicado a la Cadena de bloques.

La cadena de bloques al momento de escribir este trabajo 22 de mayo del 2017 pesa 117 GB con una altura de 468467 bloques, y un tamaño promedio de 998KB por bloque.

1.4 Proceso de minería.

La minería es el proceso similar que acuñar dinero físico, es la única forma de generar nuevos Bitcoins. La minería consiste en solucionar la prueba de trabajo de un bloque por lo cual se obtiene una recompensa en nuevos Bitcoins, este es el incentivo que mantiene la inversión de poder computacional para solucionar las pruebas de trabajo de los bloques. Además, ganan comisiones por cada transacción que añaden a un bloque que minan.

La minería previene transacciones fraudulentas y el doble gasto dentro de la cadena de bloques aumentando su tamaño y haciendo más difícil el cambio en transacciones previas.

El promedio de minado de un bloque es aproximadamente 10 minutos. El valor del incentivo por bloque minado inicio en 50 BTC en enero del 2009, es manejado por un algoritmo decreciente que se reduce a la mitad de la recompensa cada 210000 bloques, hasta el año 2140 que no existirá el incentivo o no se emitirán más Bitcoins y solo se obtendrán beneficios de las tasas sobre las transacciones.

1.5 La Red Bitcoin.

La red bitcoin tiene una topología plana colaborativa que permite interactuar los nodos completos en igualdad de condiciones para el intercambio de bloques y transacciones. Los nodos pueden ser Nodos Completos, *Simplified Pay Verification* (SPV) y mineros. La red tiene esta estructura debido a su concepción como un esquema de dinero par a par sin un ente central de confianza. Este protocolo permite propagar las transacciones para que sean registradas en la cadena de bloques.

1.5.1 Funcionamiento de red de un nodo.

El protocolo de descubrimiento de nodo al inicio no conoce que direcciones *Internet Protocol* (IP) están corriendo el protocolo bitcoin. Por lo

tanto, usa una técnica de semillas basada en *Domain Name Service* (DNS) y otra de lista de IPs conocidas. Servidores DNS son pre configurados en el cliente de referencia los cuales contienen listas de IPs con nodos completos para conectarse [9].

Los semilleros DNS son mantenidos por la comunidad y son servidores que corren el código *bitcoin-seeder* [10] y son implementaciones pre configuradas de BIND.

Para iniciar conexión necesita una IP al menos e intentará realizar conexión al puerto *Transfer Control Protocol* (TCP) 8333 por defecto, de igual manera escuchará en el puerto 8333 para esperar conexiones. Se establece un *handshake* donde el primer paso será un mensaje de versión donde se intercambiará: versión del protocolo de red P2P, lista de servicios locales, tiempo actual, la IP del nodo remoto tal como la ve el nodo local, la IP del nodo local tal como la ve el nodo remoto, la subversión del cliente bitcoin y la altura de la cadena de bloques del nodo local. El segundo paso es que el nodo remoto envíe su mensaje VERSION. Luego de esto los dos nodos deben enviar un mensaje VERACK que especifica que la conexión se estableció satisfactoriamente.

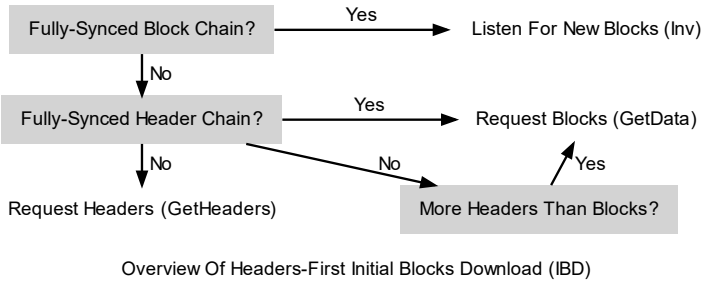
Un nodo que establece conexión puede enviar su dirección a sus vecinos con un mensaje ADDR para volverse un nodo conocido. Así mismo, puede enviar un mensaje GETADDR para obtener la lista de los vecinos de sus vecinos.

La conexión de red se mantendrá gracias a un mensaje que se envía cada 30 minutos para establecer si un nodo sigue levantado, si el nodo no responde por más de 90 minutos se asume que está fuera de servicio y se lo saca de la lista de vecinos.

Con una conexión de red establecida el siguiente paso es obtener una copia de la cadena de bloques. El cliente de referencia solo viene con el bloque#0 Génesis por defecto escrito en el código. Por tanto, el nodo ejecuta el método *Initial Block Download* (IBD) que puede usar dos esquemas para bajar la cadena de bloques *Block-First* (hasta el cliente v0.9.3) y *Header-First* (para clientes v0.10 en adelante).

El método *Header-First* primero verifica si tiene sincronizada la cadena de bloques, para esto sirve el campo Altura de la cadena del mensaje VERSION inicial. Selecciona unos de sus nodos remotos y lo elige como nodo de sincronización. Como solo tiene el bloque Génesis solicita la máxima cantidad de *headers* usando el mensaje GETHEADERS tal como muestra la figura.

Figura 1.15 Esquema Header-First para IBD



Overview Of Headers-First Initial Blocks Download (IBD)

Fuente: [2]

El nodo local arma un mensaje GETHEADERS con el único hash del bloque Genesis. El nodo remoto revisa que ese ID de bloque pertenece al bloque 0 y envía la máxima cantidad de *headers* (2000). Con lo cual el nodo local puede ir validando los primeros 2000 *headers* de bloque e ir requiriendo recursivamente, con lo cual en poco tiempo tendría los identificadores de la cadena de bloques completa. El nodo local ahora puede requerir los bloques a sus nodos remotos con la restricción de 16 bloques por vecino y con hasta 8 conexiones TCP de salida, así mantiene el rendimiento de sus nodos remotos y puede establecer paralelismo para la bajada.

El protocolo de red bitcoin tiene además actividades básicas como: toda nueva transacción debe propagarse, todo nodo debe recolectar transacciones en un bloque, cada nodo trabaja en una prueba de trabajo para minar el bloque, si el nodo soluciona la prueba de trabajo emite el bloque a todos los nodos conectados, todo nodo acepta un bloque si todas sus transacciones son válidas y no se han gastado aún, un nodo acepta un bloque que recibe como válido si comienza a trabajar en la próxima prueba de trabajo usando el hash del bloque recibido como el identificador previo [3].

1.5.2 Nodo Completo.

Este tipo de nodos fue el primero en usarse y se trata de un nodo que corre los cuatro protocolos: Cadena de bloques, Minería, Billetera y Enrutamiento de red. Este tipo de nodos es ejecutado por el cliente de referencia “Bitcoin Core 0.14.1” [2]. Al cargar toda la cadena de bloques ocupa mucho espacio en disco para almacenar todos los bloques minados por la red, porque debe mantener actualizada su copia de la cadena de bloques con todas las transacciones. Al momento de escribir este trabajo el peso total de la cadena de bloques es de 65 Gigabytes aproximadamente. Así mismo, cuando se corre el protocolo de minado también tiene un alto consumo de CPU, porque intenta realizar el minado de bloques. Se debe recordar el consumo de memoria para mantener todas las UTXO sin gastar. Este tipo de nodos puede verificar y reconstruir transacciones sin recurrir a ningún otro nodo en la red.

1.5.3 Nodo de Verificación de pago simplificado o SPV.

El uso de la tecnología móvil tiene limitación de recursos y disponibilidad de billeteras, para estos dispositivos se implementó los nodos SPV que mantienen los siguientes protocolos activos: Billetera y una variación de la cadena de bloques. Aclarando, es una variación debido a que solo mantiene las cabeceras de los bloques y no las transacciones, para conseguir un ahorro de espacio, pero pierde seguridad al no poder verificar una UTXO desde el bloque Génesis. Adicional, no mantiene una base de todas las UTXO disponibles para gastar y debe confiar en los nodos conectados para obtener vistas parciales de la cadena de bloques.

Al consultar las UTXO sin gastar pertenecientes a las llaves públicas el nodo SPV realiza consultas específicas y debilita la seguridad al exponer las claves públicas de la billetera. Este tipo de nodos es susceptible a un ataque de segmentación de red. Para mejorar la confidencialidad de las llaves públicas de la billetera se implementaron los filtros *Bloom* [11], que es una medida probabilística que permite obtener la data necesaria sin revelar las claves públicas específicas de la billetera y son distribuidos a los nodos conectados para que solo envíen las transacciones interesantes al nodo SPV.

2. Revisión de conceptos de la Cadena de Bloques

2.1 Evolución de la Cadena de Bloques

Ya se revisó en la sección de Bitcoin una descripción breve de la Cadena de Bloques relacionado con Bitcoin. Este capítulo está dedicado a revisar al detalle esta tecnología y su concepto hoy en día:

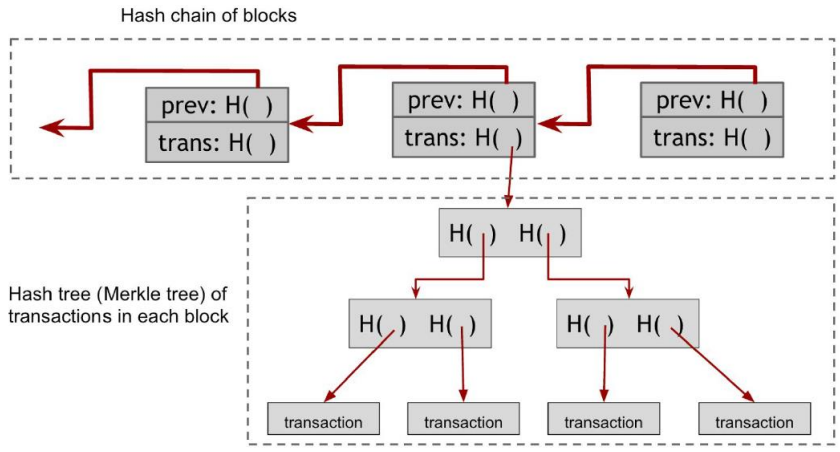
Una cadena de bloques es un libro electrónico digital compartido que registra transacciones en una red peer-to-peer pública o privada. Distribuida a todos los nodos miembros de la red, el libro registra permanentemente, en bloques, el historial de los intercambios de activos que tienen lugar entre los pares en la red [12].

Esté concepto emitido por IBM en el 2016 es el que mejor se ajusta a la realidad de la tecnología de Cadena de Bloques actual, donde el protocolo de red es parte del Blockchain en conjunto con sus reglas y tareas.

2.2 Estructura de la Cadena de Bloques.

La cadena de bloque consta de dos estructuras principales: los bloques en secuencia enlazados hacia atrás y las transacciones. En la primera estructura los bloques se enlazan hacia atrás a través del hashing SHA256 de las cabeceras, es decir todo bloque apunta al hashing de la cabecera anterior. En la segunda estructura la cabecera mantiene un hashing SHA256 de todas las transacciones a través de un árbol de Merkle, tal como se muestra en la figura:

Figura 2.1 Estructura de Hashing en la cadena de bloques. Hashing de encadenamiento de bloques y Hashing de árbol de Merkle.



Fuente: [8]

Este par de estructuras usan la función de *Hashing* y el encadenamiento en el tiempo para asegurar la integridad de los datos. Por ejemplo, para cambiar el valor de una transacción de 1 a 1000 en un bloque "v" deberá cambiarse la raíz del árbol de Merkle que viene incluido en la cabecera y el hash del bloque "v", adicional deberá cambiarse todos los hashes de las cabeceras de los bloques posteriores v+1, v+2, … hasta el último bloque de la cadena lo cual supone un esfuerzo computacional. A esto debe añadirse que cada bloque posee en la cabecera una prueba de trabajo que se realiza con el contenido de la cabecera del bloque.

2.2.1 Estructura de la cabecera del bloque

La cabecera de un bloque se compone de 80 bytes con 6 campos principales: VERSION indica el conjunto de reglas con el cual debe tratarse el bloque, PREV_BLOCK indica el hash del bloque anterior o padre, MERKLE_ROOT indica el hash de la raíz del árbol de Merkle, TIMESTAMP que es el *unix timestamp* del bloque, BITS indica la dificultad de la prueba de trabajo, NONCE indica el dato arbitrario con el cual se solucionó el reto. El campo TXN_COUNT siempre va configurado en 0.

Figura 2.2 Campos de la cabecera de bloque en bytes.

Field Size	Description	Data type
4	version	int32_t
32	prev_block	char[32]
32	merkle_root	char[32]
4	timestamp	uint32_t
4	bits	uint32_t
4	nonce	uint32_t
1	txn_count	var_int

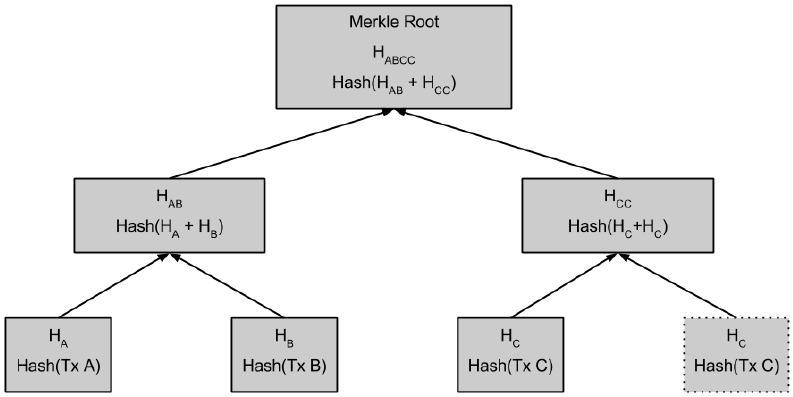
Fuente: [10]

2.3 Árbol de Merkle.

Un árbol de Merkle es una estructura binaria que se usa en la cadena de bloques para obtener un resumen de todas las transacciones incluidas en un bloque. En consecuencia, permite realizar una comprobación rápida si una transacción es parte de un bloque y no ha sido modificada.

Se construye ordenando las transacciones en una lista y se procede a contarlas para comprobar si son número par, si no es el caso se repite la última transacción. Luego se realiza *hashing* de cada transacción; se serializan los *hashes* en pares y se vuelve a realizar *hashing* recursivamente hasta obtener la raíz del árbol o raíz de Merkle como se puede observar en la figura abajo:

Figura 2.3 Construcción de un árbol de Merkle



Fuente: [8]

El *hashing* usado en este árbol es un doble SHA-256 y entrega como resultado una cadena de 32 bytes. Esta estructura permite comprobar en el orden de $Log_2(N)$ si un dato es miembro del árbol, donde N es el número de transacciones. Por ejemplo, si desea saber si la Tx A es parte del bloque, lo único que se necesitará es la raíz del árbol de Merkle y el path correspondiente H_b, H_{cc}, de tal forma que con dos operaciones se puede comprobar la membresía de la Tx A para la figura anterior. En conclusión, es eficiente para comprobar membresía de un dato tal como se muestra en la figura.

Figura 2.4 Eficiencia de un árbol de Merkle

Número de transacciones	Tamaño aprox. del bloque	tamaño de ruta (hashes)	Tamaño de ruta (bytes)
16 transacciones	4 kilobytes	4 hashes	128 bytes
512 transacciones	128 kilobytes	9 hashes	288 bytes
2048 transacciones	512 kilobytes	11 hashes	352 bytes
65.535 transacciones	16 megabytes	16 hashes	512 bytes

Fuente: [8]

Para la cadena de bloques 2.0 como se conoce a la implementación de Ethereum se usan 3 árboles de Merkle, el de las transacciones habitual en

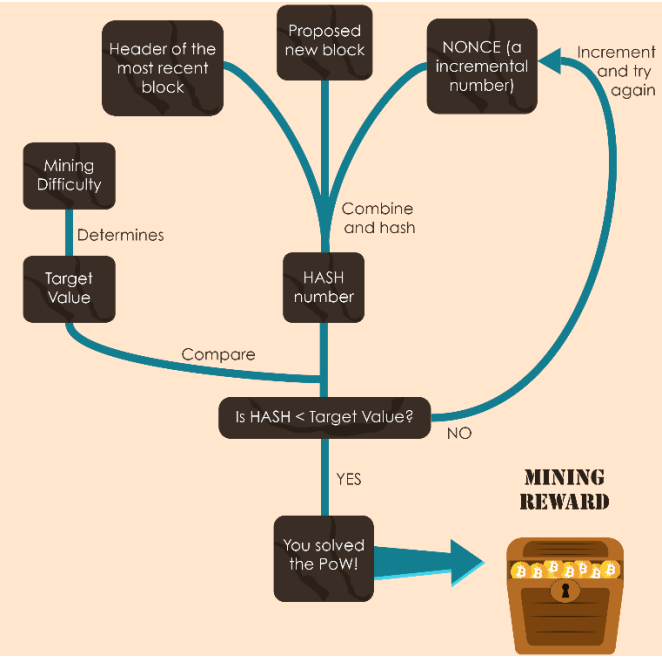
Bitcoin, uno de recipientes o cuentas, y por último uno de estados. No solo, Ethereum usa 3 árboles debido a que su visión es general y guarda otro tipo de información aparte de transacciones. Además, su visión no es una cadena de transacciones, sino que tiene el marco conceptual de manejo de saldos por cuenta o recipiente. El árbol que usan se denomina Merkle Patricia Tree [13].

Otros proyectos como Multichain [14] se especializan en cadena de bloques privadas y mantienen la misma arquitectura de Bitcoin Core, pero con pequeñas adaptaciones en el protocolo de red par a par para brindar privacidad.

2.4 Prueba de trabajo y Minería.

La PoW es un reto a ejecutar por un nodo minero para unir un bloque verificado a la cadena de bloques. El incentivo del minero es que recibirá Bitcoins por su gasto de recursos para resolver el reto, como se muestra a continuación en la figura:

Figura 2.5 Prueba de trabajo



Fuente: [15]

La prueba de trabajo ejecutada por la red Bitcoin es ejecutada de acuerdo con una complejidad o *Target*, el reto del minero es realizar un hash SHA256 de un *string* serializado compuesto por el *header* del bloque más las

transacciones y lograr obtener un valor *hashing* por debajo de la complejidad propuesta o valor objetivo. Tal como mostramos en la formula a continuación:

SHA256(SHA256(cabecera del bloque)) < objetivo del reto

El espacio de salida de la función hash es 2^{256} y para lograr el objetivo del reto el resultado del hash debe caer en un espacio mucho menor propuesto por la complejidad o valor objetivo del reto.

Para lograr un valor que solucione el reto se debe variar el campo NONCE de la cabecera del bloque. Cada minero puede usar su propia plantilla para variar el NONCE de 4 bytes y conseguir solucionar el reto.

Este reto tiene tres propiedades. La primera es su dificultad computacional: El reto debe ser difícil de computar y todos los nodos completos conocen el *Target.*

La segunda es Costo variable: El *Target* se recalcula cada 2016 bloques y lo hace de acuerdo al tiempo que se tardó en minar los últimos 2016 bloques, de tal forma que si demoro en procesar más de 10 minutos el promedio de minado por bloque se decrementa la complejidad del objetivo y si se tardó menos se incrementa la complejidad del objetivo.

La tercera propiedad es ser fácilmente verificable: Cuando un nodo soluciona el reto envía el bloque completo a los demás nodos, así reciben el NONCE (número que soluciona el reto) y BITS (dificultad), con estos datos se puede verificar si efectivamente el hash del header soluciona el TARGET propuesto en BITS.

Ahora como se mencionó existe un incentivo para el minero que solucione el reto y es una cantidad de Bitcoins, este proceso es la analogía para acuñar monedas físicas. Los incentivos están configurados de forma geométricamente decreciente para emitir máximo 21.000.000 BTC. El número máximo de moneda circulante fue configurada por Satoshi podría ser cualquier otro número. De tal forma que para el año 2140 se terminaría de emitir el ultimo Bitcoin con una altura de 6.930.000.

Los ciclos de incentivos están configurados de tal forma que cada 210.000 bloques o 4 años aproximadamente se decrezca en la mitad del valor del incentivo iniciando con un valor inicial de 50BTC el 3 de enero del 2009 con el minado del bloque Génesis realizado por Satoshi Nakamoto.

Ahora, como se puede observar el proceso de minería será menos rentable en el tiempo ya que demandará más poder computacional y energía eléctrica. Sin embargo, existen las diferencias entre los VOUT y VIN en las transacciones que son los costos que pagan las transacciones por ser incluidas en un bloque para minar y que están relacionadas con la longitud de la transacción.

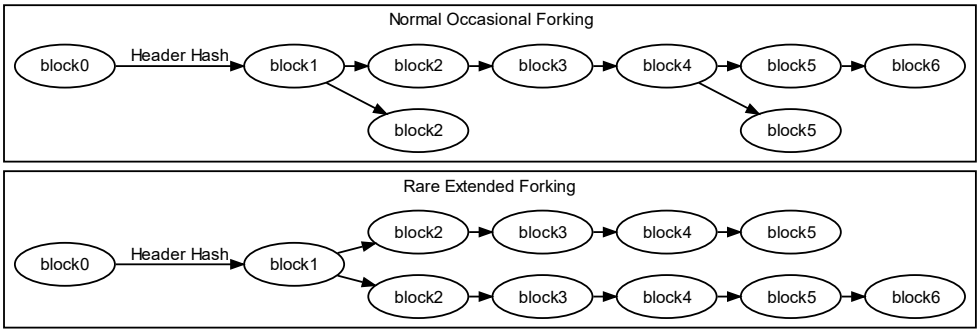
2.5 Consenso de la red

El consenso de la red se refiere a la capacidad de prevenir el doble gasto y evitar la bifurcación de la cadena de bloques. A continuación, veremos los casos:

2.5.1 Bifurcación o *fork* por minado simultáneo

Cualquier minero puede lograr superar el reto de la prueba de trabajo y minar un bloque, entonces se puede dar la situación que dos mineros emitan un bloque de una determinada altura casi simultáneamente como mostraremos en la figura

Figura 2.6 Bifurcación ocasional por minado simultaneo.



Fuente: [2]

Las bifurcaciones cortas son sencillas de solucionar por las reglas de consenso o selección de los nodos que eligen la cadena más larga o

trabajada, es decir en algún instante uno de los ramales obtendrá más bloques o garantizará más trabajo sobre la cadena y la rama más corta se desechará cuando existan este tipo de forks. Cuando se producen estos forks los nodos deben mantener las dos cadenas. Las bifurcaciones largas son raras de producir por minado simultáneo, se podría ver como un ataque del 51% del poder computacional de la red bitcoin. En otras palabras, se trata de mineros honestos tratando de trabajar la cadena original y mineros deshonestos tratando de crear una cadena falsa o con sus valores. El caso de bifurcación larga tiene otros orígenes que explicaremos abajo.

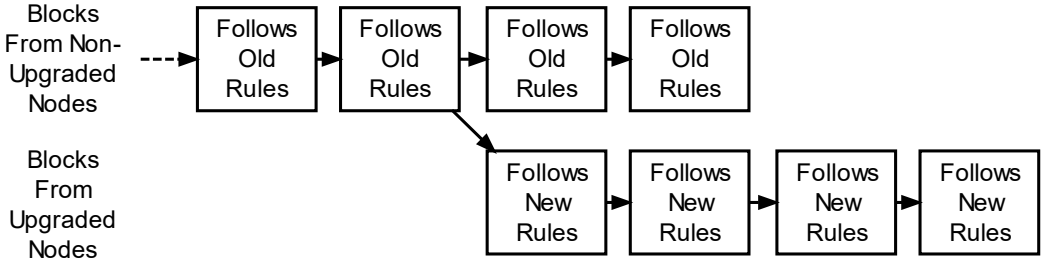
2.5.2 Bifurcaciones suaves y bifurcaciones duras.

También conocidos como *soft fork* y *hard fork*, estos se producen por cambios en las reglas de consenso que manejan los nodos.

Todos los nodos usan las mismas reglas de consenso para validar los bloques de la cadena. Estas reglas se cambian para soportar nuevas características o prevenir el abuso de la red o ataques por nodos deshonestos. Cuando se implementan los cambios existe una ventana de tiempo donde hay nodos actualizados siguiendo las nuevas reglas y nodos desactualizados siguiendo las viejas reglas. Esto crea dos escenarios posibles: el *hard fork* y el *soft fork*

Un bloque emitido desde un nodo actualizado es aceptado por los nodos actualizados pero rechazados por los nodos desactualizados. Un ejemplo de este caso es activar una nueva característica dentro del bloque, de tal manera que los nodos actualizados aceptarán el bloque minado pero los nodos desactualizados lo rechazarán porque no respeta sus reglas. Este caso se conoce como bifurcación dura o hard fork, donde el grupo de nodos actualizados mantendrá una cadena de bloques con nuevas reglas y otro grupo de nodos desactualizados mantendrá una cadena de bloques con las viejas reglas indefinidamente como se puede ver en la figura abajo.

Figura 2.7 Caso de un hard fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

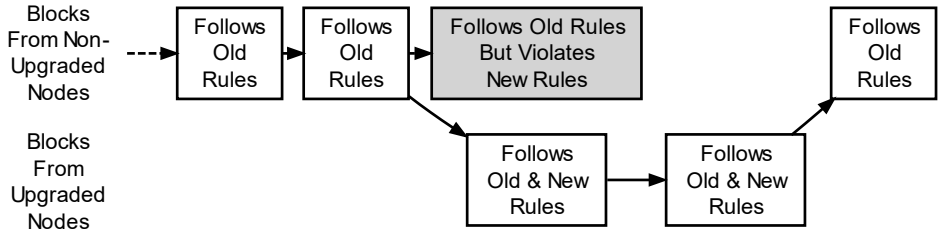
Fuente: [2]

El hard fork también es conocido como *not forwards-compatible* lo cual significa que ningún nodo con la versión antigua de software aceptará un bloque emitido con la nueva versión. Ante este caso todos deben actualizar sus programas de Bitcoin: mineros, comercios, billeteras, etc.

Este caso es peligroso por la cantidad de transacciones que se pueden perder o reflejar sobre una cadena y no sobre otra. Este caso particular sucede en el momento de escribir este trabajo, el 31 de julio se activarán algunas características y modificaciones sobre la red Bitcoin que generará un hard fork. Para este hard fork se planea aumentar el tamaño del bloque de 1MB a 2MB lo que hará romper la red Bitcoin en dos cadenas. [2]

El otro posible escenario se conoce como soft fork y se produce cuando se activa alguna característica que limita funcionalidad o restringe de posibles ataques, manteniendo la compatibilidad hacia atrás. Es decir, un bloque emitido por un software de minería desactualizado y que rompe las reglas del nuevo software será rechazado por nodos actualizados, igual se crearán dos cadenas por las partes actualizadas y desactualizadas de la red. El éxito de un soft fork es que al menos el 51% de los mineros se encuentren actualizados de tal forma que la cadena con los bloques actualizados crecerá más rápido y será aceptada por los nodos desactualizados como se puede observar en la figura.

Figura 2. Soft fork



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

Fuente: [2]

En este caso los mineros se ven forzados a actualizar, mientras los nodos de usuarios o billeteras pueden seguir funcionando sin actualizar. También se conoce como forwards-compatible que significa que los nodos sin actualizar seguirán aceptando nuevos bloques minados por mineros con software actualizado. La red Bitcoin ha experimentado varios soft forks desde su creación, así mismo hubo un caso de un soft fork que se volvió hard fork y los desarrolladores tuvieron que realizar un downgrade de funcionalidad sobre los nodos actualizados para mantener una sola cadena de bloques.

2.6 Características principales de la Cadena de Bloques.

Una vez que hemos estudiado Bitcoin que es una aplicación particular de la cadena de bloques, ahora podemos indicar sus principales características que fueron citadas por Halamka en el 2017 [16]:

Base de datos distribuida. Cada nodo en una cadena de bloques tiene acceso a toda la base de datos y su historial completo. Además, ninguna de las partes controla los datos y puede verificar los registros de sus pares directamente, sin un intermediario.

Transmisión punto a punto. La comunicación ocurre directamente entre pares sin pasar por un nodo central. Y cada nodo almacena y envía la información a todos los otros nodos.

Transparencia con el seudo anonimato. Cada transacción y su valor asociado son visibles para cualquier persona con acceso al sistema. Cada nodo (en el caso de un minero) o usuario en una cadena de bloques puede tener una o más direcciones alfanuméricas de 30 caracteres que la identifica.

Los usuarios pueden elegir permanecer en el anonimato o proporcionar una prueba de su identidad a otros. Las transacciones ocurren entre las direcciones de cadenas de bloques.

Registros no modificables en el tiempo. Una vez que se ingresa una transacción en la base de datos y la cadena de bloques se actualiza, los registros no pueden ser alterados, ya que están vinculados a cada bloque hacia atrás. Se utilizan diversos algoritmos y enfoques computacionales para asegurar que el registro en la base de datos sea permanente, ordenada cronológicamente y disponible para todos los demás en la red.

Lógica Computacional. La naturaleza digital del libro mayor significa que las transacciones de la cadena de bloques pueden estar ligadas a la lógica computacional y en esencia programadas. Así, los usuarios pueden configurar algoritmos y reglas que activen automáticamente las transacciones entre nodos usando las reglas de script.

2.7 Criterios de selección de la Cadena de Bloques como una solución

La cadena de bloques es una tecnología disruptiva que puede aplicarse para solucionar algunos problemas como el registro de eventos, criptomonedas, manejo de datos, contratos inteligentes, manejo de identidades, seguimiento de productos y cientos de soluciones. Posee las siguientes características que deben analizadas como ventajas o desventajas antes de ser aplicable a cualquier problema.

2.7.1 Ventajas de la Cadena de Bloques como una solución

a) Invariancia en el tiempo. Todo dato o hashing de datos ingresado en la cadena se va a mantener sin modificación en el tiempo. Esta característica permite establecer una marca del paso de tiempo sobre la información o un registro histórico invariable. Puede ser aplicable en varios campos como salud, gobierno público, financiero, ciencias donde se requiera registrar un dato sin variación en el tiempo.
b) Anonimato. Al usar la autenticación basada en direcciones aleatorias generadas por el usuario se puede establecer un seudo anonimato basado en la firma digital y con la posibilidad de dar a

conocerse si el usuario lo permite. Esto sirve para establecer un sistema de privacidad donde se mantenga reservado la identidad de los usuarios del sistema.

c) Independencia de ente central de confianza. El consenso de la red resuelve el problema de dependencia de una entidad de confianza. En el campo financiero apoya a los costos de micro transacciones que en los sistemas actuales están limitadas por los costos de los intermediarios que proveen la confianza a la red. En otros campos es una fortaleza poder usar el consenso de una red distribuida en lugar de la dependencia de un punto central.

2.7.2 Desventajas de la Cadena de Bloques como una solución

a) Anonimato. Puede ser una desventaja en usos financieros tradicionales, se puede ver como un posible foco de incidencias debido a las leyes KYC *Know Your Customer.* La legislación actual de la mayoría de países exigen a los sectores financieros cumplir con la ley de conocer al cliente para evitar el lavado de activos.
b) Cantidad de transacciones. Esto se evidencio en el 2017 al tener una alta tasa de transacciones que no se minaban por no entrar en el tamaño de bloque de 1MB, esta limitante se corrigió al ampliar el bloque a 2MB.
c) Datos en el bloque. El uso particular de la cadena de bloques en Bitcoin usa el dato dentro de cada bloque, entiéndase como dato los valores en Satoshis. Sin embargo, en otras soluciones debe usarse un esquema en el cual el dato sea grabado en otra base por fuera de la cadena y lo que se registre en la cadena sea el hash del dato grabado en la base. O en su caso modificar el protocolo para hacer un bloque de tamaño variable.
d) Tiempo de respuesta. El protocolo de red P2P usado por la cadena de bloques usa un algoritmo de consenso que emite bloques en cierto promedio de tiempo, por tanto si una aplicación necesita tiempos en milisegundos es poco probable que la cadena de bloques sea la solución buscada.

2.7.3 Temas para considerar en la Cadena de Bloques como una solución.

Los siguientes puntos no son pros o contras de la cadena de bloques, pero son temas para considerar en cualquier aplicación de esta tecnología.

a) Minería e incentivos. En una solución de criptomoneda la minería es una tarea atractiva debido al incentivo de recibir criptomoneda por el esfuerzo computacional de solucionar el reto, para otras soluciones esto puede ser una desventaja al no ser un incentivo financiero. Por tanto, se debe analizar bien un esquema de incentivos para mantener la red de mineros.
b) Red par a par. Para soluciones que requieran ser eficientes en el recurso del tiempo de propagación de datos esto puede ser un problema. Ya que la estructura de la red y las reglas de consenso no garantizan que una transacción o evento sea incluido en un bloque para ser minado. En consecuencia, no se puede garantizar un tiempo de asentamiento del dato en el registro histórico.
c) Llaves criptográficas. En ciertas aplicaciones se requiere de un ente central o gobierno para entregar o generar las llaves criptográficas a cada usuario que sea enrolado. Se debe tener en cuenta cómo solucionar el enrolamiento de los usuarios a la red.
d) Almacenamiento de datos. En Bitcoin la base es distribuida y replicada en todos los nodos lo cual consume almacenamiento. En aplicaciones que tengan almacenamiento pesado e intensivo se debe analizar la estrategia de mantener una base centralizada o distribuida externa a la cadena solo en ciertos nodos para no hacer pesada la cadena de bloques.

2.8 Otras versiones de Cadenas de Bloques.

Existen algunas versiones nuevas de la cadena de bloques que hacen cambios al modelo conceptual, a las pruebas de trabajo y a los árboles de Merkle, tales casos son Ethereum: Blockchain 2.0 y ALGORAND: The True Public Ledger. Nuestro trabajo explica brevemente Ethereum, pero no va a

dar una explicación al detalle debido que nos centramos en explicar la cadena de bloques pura creada por Nakamoto.

En el 2014 Vitalik Buterin, Gavin Wood y Jeffrey Wickle [13] lanzaron el proyecto Ethereum que se basaba en una evolución de la cadena de bloques con características programables, es decir, que en lugar de llevar transacciones llevaba código, lo cual permite darle cualquier uso imaginable a la cadena de bloques. La iniciativa Ethereum se puso como objetivo el establecimiento de Contratos Inteligentes pero su código Turing completo puede permitirnos programar cualquier otra aplicación sobre una única cadena de bloques. Para lograrlo Ethereum cuenta con los siguientes componentes:

a) Código Turing Completo. Programación que se puede insertar en una transacción de Ethereum, con característica de un Turing completo, es decir permite bucles y lógica de programación compleja. Existen compiladores para escribir el código en JavaScript, Python y Go. Este código se conoce como contrato inteligente.
b) *Ethereum Virtual Machine* (EVM). Para poder ejecutar el código cargado sobre la cadena de bloques todos los nodos deben correr un EVM que es una máquina virtual que ejecuta el código dentro de cada bloque.
c) Red par a par. Al igual que Bitcoin, Ethereum corre sobre una red P2P donde todos los nodos ejecutan la EVM que aseguran el consenso de la red y niveles de tolerancia antes fallas.
d) *Account* o Cuenta. Ethereum hace cambio al modelo conceptual de Bitcoin al no tener como unidad básica la transacción. Su unidad es la Cuenta la cual es la clave primaria, la cadena de bloques mantiene registro constante de cambios sobre una cuenta, así mismo se transfiere valor entre cuentas. Las cuentas pueden ser *External Owned Account* (EOA) o *Contract Account* (CA), las primeras permiten crear las segundas. Las EOA son creadas por los usuarios para establecer contratos y clausulas las cuales se

programan sobre las CA, ese código establece el contrato inteligente y se ejecuta al enviar transacciones a las CA.

e) Minería. Se mantiene el mismo concepto de Bitcoin y el que envía transacciones debe pagar por cada línea de código que envié a ejecutar. Los pagos en vez de usar Satoshis o Bitcoins usan Ether que es el token de Ethereum. Así mismo, cada nodo recibe, verifica, ejecuta y transmite transacciones en bloques minados hacia los otros nodos.

f) Prueba de trabajo. Ethereum usa una técnica distinta a Bitcoin. El algoritmo de prueba de trabajo emplea el bus de memoria RAM para eliminar el monopolio que se puede generar por la prueba de trabajo basado en esfuerzo de CPU. Todo esto para eliminar el problema de minería basada en CPU como pasa en Bitcoin garantizando una distribución descentralizada de la minería.

2.9 La primera Cadena de Bloques resistente a ataques cuánticos

El 29 de mayo del 2017 el *Russian Quantum Center* anunció la creación de la primera cadena de bloques asegurada cuánticamente [1] o resistente a ataques de computación cuántica. El trabajo explica que dos funciones clave, hashing SHA2 y firma digital ECDSA [4] son comprometidas por una computadora cuántica.

El algoritmo cuántico de Shor resuelve la factorización de enteros y el problema del logaritmo discreto en tiempo polinomial lo cual afectaría al protocolo ECDSA. Por otro lado, el algoritmo de búsqueda de Grover permite la aceleración cuadrática en el cálculo de la función de hash inversa que debilita el SHA2. En consecuencia, esto va a permitir un ataque del "51%", es decir, la mayoría de la potencia de la red sería manejado por nodos maliciosos monopolizando la minería.

El trabajo de los rusos explica el uso de un esquema de firma post cuántico podría prevenir el problema del doble gasto, pero no previene los ataques de minado al usar una computadora cuántica para ganar la carrera de emisión de bloques lo cual dejaría la red monopolizada. Además, los algoritmos post cuánticos actuales se basan en suposiciones no probadas.

Esta nueva versión cuántica segura propone el uso de una red cuántica punto a punto por cada par de nodos para el uso de QKD y otra red clásica para enviar mensajes con tags de autenticación creados a partir de claves privadas generadas en la red QKD. Lo que se pretende es usar QKD para que cada par de nodos puedan lograr autenticación más el uso de algoritmos clásicos de consenso para reemplazar el uso de firmas digitales. Para este caso usan al algoritmo de Shostak, Lamport and Pease [17] que permite alcanzar un acuerdo bizantino en cualquier red con una comunicación autenticada por pares, siempre y cuando el número de partes deshonestas sea menor que n/3, donde n es el número de nodos.

Esta implementación aún tiene algunos puntos que resolver como el uso intensivo de datos, el establecimiento de canales cuánticos por pares y la complejidad para que un nuevo nodo se levante en la red o reingrese después de una caída.

3. Análisis de aplicabilidad de la Cadena de Bloques como solución para la gestión de registros de salud electrónicos de pacientes en el campo de la salud.

3.1 Breve revisión de Historias Clínica Electrónica.

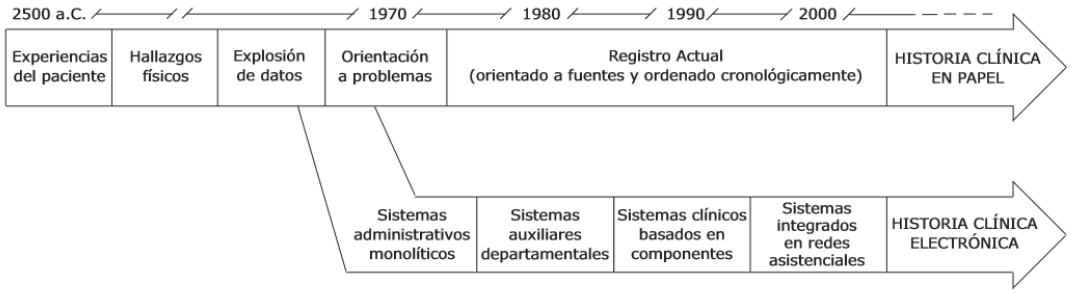
La *International Standard Organization* (ISO) define un *Eletronic Health Record* (EHR) como un “repositorio de información sobre el estado de salud de un sujeto de cuidado, en forma procesable por computadora” [18]. Esta definición la mejoran Gunter y Terry como “…un concepto evolutivo definido como una colección longitudinal de información de salud electrónica sobre pacientes individuales y poblaciones principalmente, será un mecanismo para integrar la información de atención médica actualmente recopilada en los registros médicos en papel y electrónicos con el propósito de mejorar la calidad de la atención” [19]

Para complementar un *Eletronic Medical Record* (EMR) es definido como registro electrónico medico creado por un proveedor de servicios u hospital y que puede ser el origen de datos para un EHR. Otro origen de datos puede ser un *Personal Health Record* (PHR) que es un aplicativo de recolección de datos de salud manejado por el paciente y que puede proporcionarse a un agente de salud.

Entonces en este trabajo vamos a usar el término EHR por ser de uso más amplio, con múltiples orígenes de datos, de uso interinstitucional y alcance geográfico nacional. En nuestro idioma se usa indistintamente los términos historia clínica electrónica o registro médico electrónico o registro de salud electrónico.

Hace 2500 años en la antigua Grecia el registro se basaba en las vivencias de los enfermos de acuerdo con Hipócrates. Todo se basaba en la observación de los pacientes. Con el progreso se obtuvieron nuevos instrumentos de medición que ayudaron a completar la historia con las mediciones del médico. Luego con la aparición de exámenes, imágenes hubo más diversidad de fuentes de información para aportar al registro. En el último siglo se estructuró la información orientándola hacia una fuente y se ordenó cronológicamente para dar paso a la historia clínica como se muestra en la figura. [20]

Figura 3.1 Evolución de la historia clínica



Fuente: [21]

Ahora las capacidades claves de un EHR se identifican primero por los usos como se explica en la siguiente tabla:

Figura 3.2 Usos de un EHR

Usos Primarios y Secundarios de un EHR	
Usos Primarios	Usos Secundarios
- Cuidado del paciente	- Educación
- Gestión del cuidado del paciente	- Regulación
- Procesos de apoyo al cuidado del paciente	- Investigación
- Financieros y otros procesos administrativos	- Salud Pública y Seguridad Nacional
- Autogestión del paciente	- Apoyo a la política

Fuente: [22]

Los usos primarios son diseñados para el núcleo del Sistema EHR y tiene que ver con los cuidados del paciente y parte administrativa como gastos, además de los datos provenientes de un PHR. Los usos secundarios sirven para la educación, investigación y la administración de nuevas políticas de salud basados en la información generada por el sistema EHR. Una vez que tenemos estas categorías de usos podemos definir las capacidades de un EHR como se muestra a continuación [23]:

Figura 3.3 Capacidades claves de un EHR

Funcionalidades principales para un EHR	
- Información y datos sobre salud	- Soporte al paciente
- Gestión de resultados	- Procesos administrativos
- Órdenes de ingreso y gestión	- Informes y gestión de la salud de la población
- Apoyo a las decisiones	
- Conectividad y comunicación electrónica	

Fuente: [23]

Información de salud son datos propios del paciente proporcionados por el médico o cualquier proveedor de salud.

La administración de resultados se preocupa del manejo electrónico de todo tipo de exámenes de laboratorio, imágenes, etc. El manejo de resultados en línea permite reducir costos y mejorar la eficiencia de los tratamientos.

Los beneficios de órdenes computarizadas están bien documentados por su efectividad y mejoran las órdenes perdidas o con errores por escritura a mano. Al igual los sistemas de soporte en toma de decisiones han demostrado su eficacia en el desempeño clínico de muchos aspectos de la atención de salud, incluida la prevención, la prescripción de medicamentos, el diagnóstico, manejo, y detección de eventos adversos y brotes de enfermedades.

La conectividad electrónica es esencial para los sistemas EHR, especialmente para aquellos pacientes con condiciones crónicas, que tienen múltiples proveedores de salud en múltiples escenarios que deben coordinar planes sanitarios.

3.2 Problemática de los registros electrónicos de Salud.

"*Todo lo que haya visto u oído durante la cura o fuera de ella en la vida común, lo callaré y conservaré siempre como secreto, si no me es permitido decirlo*" *Juramento de Hipócrates* [24].

La EHR desde su concepción no fue diseñada para ser manejada como un documento multi institucional lo cual limita el contexto de la información a las instituciones donde se atiende al paciente.

Una arista del problema es mantener la privacidad y confidencialidad de los datos del paciente, otra arista es la propiedad sobre los datos, la pregunta sería ¿son de la institución de salud o del paciente y por último la disponibilidad e integridad de los datos del paciente sin importar la ubicación geográfica o el proveedor de servicios de salud. Aquí nos debemos formular las siguientes preguntas respecto a los datos: ¿son propiedad de la institución de salud o del paciente?, ¿Deben ser ofrecidos para investigaciones en el campo de salud sin afectar la seguridad de la información y cómo?, ¿Cómo un paciente puede llevarlos a través de toda la red de proveedores de servicios o como los proveedores deben facilitarlos entre sí?, ¿Quién garantiza la seguridad de la información o se hace responsable de la gestión de los datos médicos? A continuación, analizaremos varias posturas y conceptos de estos problemas.

Tomando un artículo especial de Gelpi, Perez y Rancich [25] del 2000 acerca de la confidencialidad en los juramentos médicos citamos "la confidencialidad, junto con los principios éticos de beneficencia y no-maleficencia, es la norma más señalada en los Juramentos Médicos de la actualidad. A pesar de ello, el avance científico-técnico en la Medicina ha hecho que constituya una de las reglas más controvertidas por sus excepciones" [25] y además "…la confidencialidad es considerada en estos tiempos como un deber moral para el bien del paciente y por respeto a su autonomía; pero a pesar de ello, en la actualidad en Medicina se está replanteando el deber de guardar el secreto en una forma absoluta" [25].

En 1995 la *National Research Council* de la *National Academy of Sciencies en Wahisngton D.C*. por solicitud de la Biblioteca Nacional de Medicina (NLM), realizó un estudio sobre el mantenimiento de la seguridad en

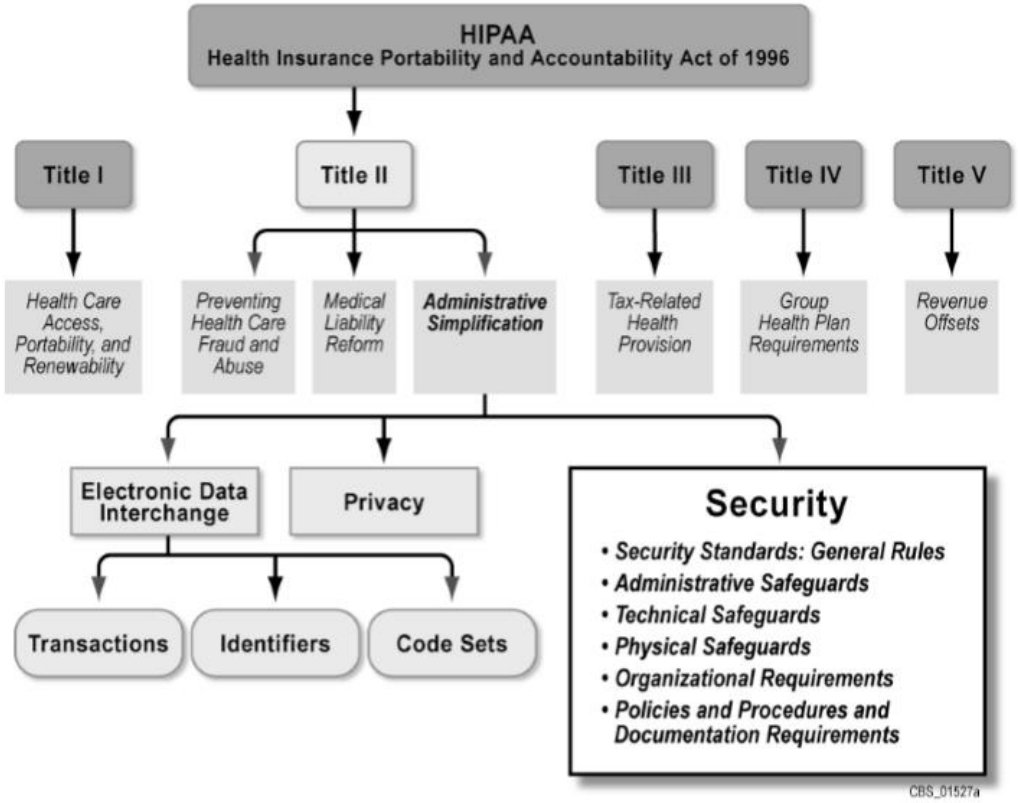
las aplicaciones sanitarias de la Infraestructura Nacional de Información (NNI), producto de lo cual en 1997 recomendó políticas y procedimientos [22] para proteger la privacidad y seguridad de los sistemas de información de atención médica. La mayor vulnerabilidad estaba relacionada con el uso inadecuado de la información por parte de los trabajadores de la salud como parte de su trabajo regular, en este mismo sentido el riesgo es mucho mayor para la información guardada en papel [22]. Donde la palabra seguridad fue usada para describir una serie de medidas que las organizaciones aplican para proteger la información y sistemas, incluye esfuerzos no sólo para mantener la confidencialidad de la información sino también la integridad y disponibilidad de esa información y de los sistemas de información utilizados para acceder a ella.

3.3 Ley de Portabilidad y Responsabilidad del Seguro de Salud de 1996

La *Health Insurance Portability and Accountability Act of* 1996 (HIPAA) o ley 104-191, protege el uso y la divulgación de la información de salud de las personas. Incluyendo disposiciones de simplificación administrativa, las cuales son requerimientos al *Human Health Services* (HHS) para adoptar estándares nacionales para transacciones y conjuntos de códigos electrónicos de atención médica, identificadores únicos de salud y seguridad. Al mismo tiempo, el Congreso reconoció que los avances en la tecnología electrónica podrían erosionar la privacidad de la información de salud. En consecuencia, el Congreso incorporó en las disposiciones de la HIPAA la adopción de protecciones federales de privacidad para información de salud individualmente identificable [26].

La HIPAA implementó las siguientes reglas de simplificación administrativa: Regla de Privacidad, Regla de Seguridad, Regla de Aplicación y Regla final de Omnibus o *Health Information Technology for Economic and Clinical Health* (HITECH). La estructura completa de HIPAA se muestra en la figura abajo.

Figura 3.4 Componentes HIPAA



Fuente: [27]

Todos los proveedores o entidades de salud cubiertos por el HIPAA están obligados a proveer el formulario de aviso de prácticas de confidencialidad con el fin de que sea leídas y firmadas. Este formulario explica los siguientes ítems:

a) Las formas en que su proveedor de salud tiene permitido usar o compartir información sobre su salud.
b) Los derechos de confidencialidad del paciente, que incluyen su derecho a obtener una copia de su historial médico, a revisarlo, a pedir que sea corregido y a quejarse si considera que ha habido alguna violación de sus derechos de confidencialidad.
c) El compromiso legal de su proveedor de cuidados para proteger la información sobre su salud.
d) Lista de contactos para obtener más información acerca de las políticas de confidencialidad de su médico o compañía de seguros.

El paciente tiene el derecho de no firmar el formulario, pero no significa que rechaza el manejo de su información, solo que no acepto firmar el aviso de prácticas de confidencialidad. El proveedor de salud solo debe guardar la constancia de que no firmo el formulario y proveer los cuidados de salud.

3.3.1 Regla de privacidad

El HHS publicó la Regla de Privacidad en diciembre de 2000 como producto del requerimiento de la ley HIPAA. La Norma de Privacidad aborda el uso y divulgación de la información de salud de los individuos denominada información de salud protegida por organizaciones sujetas a la Regla de Privacidad, las cuales se denominan entidades cubiertas. También establece estándares de privacidad para que las personas puedan entender y controlar como su información de salud es usada. El cumplimiento de la regla de privacidad fue requerido a partir del 14 de abril del 2003.

Información de Salud Protegida es toda la "información de salud identificable individualmente" que se mantiene o transmite por una entidad cubierta o su socio comercial, en cualquier formato o medio, ya sea electrónico, papel u oral. La Regla de Privacidad llama a está “información de salud protegida” o *Protected Healt Information* (PHI). La “información de salud identificable individualmente” incluye datos demográficos y se relaciona con: la salud o la condición física o mental en el pasado, presente o futuro del individuo; la prestación de atención de salud a la persona; y el pago en el pasado, presente o futuro por la prestación de servicios de salud al individuo. Es información que identifica al individuo o para el cual existe una base razonable para creer que puede ser usada para identificar al individuo. En esta información también se incluyen los nombres, direcciones, número de identificación nacional, fecha de nacimiento, etc.

Las entidades cubiertas son comunes a todas las reglas de Simplificación Administrativa y constan en la figura abajo.

Figura 3.5 Entidades cubiertas que deben cumplir con las administrativas simplificadas HIPAA

Un Proveedor de Atención Médica	Un Plan de Salud	Un Centro de Cuidado de Salud
Esto incluye proveedores como :	- Compañías de seguros de salud	Esto incluye entidades que procesan información de salud no estándar que reciben de otra entidad incluida en el estándar (Por ejemplo, formato electrónico estándar o contenido de datos) o viceversa.
- Doctores	- Organizaciones de mantenimiento de la salud	
- Clínicas		
- Psícologos	- Planes de Salud de empresas	
- Dentistas	- Programas gubernamentales que pagan por servicios de salud, como Medicare, Medicaid y los programas de atención médica militar y de veteranos	
- Quiroprácticos		
- Hogares de ancianos		
- Farmacias		
... pero sólo si transmiten información en forma electrónica sobre una conexión con transacciones para las cuales HHS ha adoptado una norma.		

Fuente: [28]

Principio de la Regla. El propósito de la regla de privacidad es definir y limitar las circunstancias en la cual la PHI de un individuo puede ser usada o distribuida por las entidades cubiertas. Una entidad cubierta solo puede usar o revelar la PHI en los siguientes casos: según lo permita o requiera la regla de privacidad y si el individuo dueño de la PHI o su representante lo autoriza por escrito.

Principio General para uso y divulgación. Una entidad cubierta tiene permitido usar y divulgar la PHI sin la autorización del individuo en los siguientes casos:

a) Al individuo. Una entidad cubierta puede revelar la PHI a la persona que es el dueño de la información.

b) Para Operaciones de tratamiento, pago y atención médica. Una entidad cubierta también puede usar y divulgar la PHI para su tratamiento, pago y otras actividades de cuidado de salud dentro de sus sistemas. Además, puede divulgar la PHI a otra entidad cubierta u otro proveedor de atención médica o actividades de pago, siempre que ambas entidades cubiertas tengan o tuvieran una relación con el individuo y la PHI.

c) Oportunidad para aceptar u objetar. El permiso informal se puede obtener preguntando al individuo abiertamente, o por circunstancias que claramente dan al individuo la oportunidad de acordar, aceptar u objetar. Cuando el individuo está inhabilitado, en una situación de emergencia, o no

está disponible, las entidades cubiertas pueden hacer usos y divulgaciones, bajo su juicio profesional, siempre y cuando sea en el mejor interés del individuo.

d) Incidente de uso y divulgación de otra manera permitido. La Regla de Privacidad no requiere que se elimine todo riesgo de uso o divulgación de PHI. Se permite el uso o la divulgación de esta información que se produce como resultado de un "incidente", siempre que la entidad cubierta haya adoptado todas las salvaguardas razonables como lo requiere la Regla de Privacidad y la información que se expuso sea lo "mínimo necesario", como lo requiere la Regla de Privacidad.

e) Actividades de beneficio e interés público. La Regla de Privacidad permite el uso y divulgación de PHI, sin autorización ni permiso de un individuo, para 12 propósitos nacionales de prioridad. La divulgación está permitida, aunque no requerida, por la regla en reconocimiento a los importantes usos de información de salud fuera del contexto de la atención de la salud. Las condiciones o limitaciones específicas se aplican a cada propósito de interés público, buscando el equilibrio entre el interés de la privacidad individual y la necesidad de interés público de esta información.

f) Conjunto de datos limitado para propósitos de investigación, salud pública y operaciones de tratamientos de salud. Un conjunto limitado de datos es PHI reducida a la cual se le han eliminado ciertos identificadores directos específicos de individuos, miembros de la familia y empleadores. Un conjunto de datos limitado puede ser usado y divulgado para investigación, operaciones de cuidado de salud y propósitos de salud pública, siempre que el destinatario celebre un acuerdo de uso de datos que prometan salvaguardas especificadas para la PHI dentro del conjunto limitado de datos.

3.3.2 Regla de Seguridad

HHS publicó la Regla de Seguridad en febrero de 2003. Esta Regla establece normas nacionales para proteger la confidencialidad, integridad y disponibilidad de la información de salud protegida electrónica también conocidos como *electronic Protected Health Information* (ePHI). El

cumplimiento de la Regla de Seguridad fue requerido a partir del 20 de abril de 2005. Sus principales objetivos son:

a) Mantener protegida la información de salud de las personas.
b) Permitir y regular el flujo de información de salud entre proveedores de salud para proveer y promover los cuidados de salud.
c) También exige que sus proveedores de atención médica, así como también su plan de salud, le expliquen sus derechos y la manera en que la información sobre su salud puede utilizarse o compartirse.

El estándar *45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule* tiene como base 3 conceptos: la norma debe ser completa para abarcar todos los aspectos de la seguridad, escalable para poder ser implementada por todas las entidades cubiertas sin importar su tamaño o tipo, y no debe estar ligada a ninguna tecnología específica para que las entidades cubiertas puedan aprovechar avances tecnológicos futuros.

Requerimientos de la regla. Los requerimientos se hacen para que una entidad cubierta pueda proteger la integridad, confidencialidad y disponibilidad de la información de salud electrónica de los individuos. Las categorías de requerimientos son: procedimientos administrativos, salvaguardas físicas, servicios técnicos de seguridad y mecanismos técnicos. En la siguiente figura se explican las categorías.

Figura 3.6 Matriz de estándares de seguridad

Matriz estándares de seguridad – Apéndice A hasta subsección C de sección 164		
Estándares	Secciones	Especificaciones de implementación (R)=Requerido, (D)= Deseable
Salvaguardas Administrativas		
Proceso de gestión de la Seguridad	164.308(a)(1)	Análisis de Riesgos (R)
		Gestión del Riesgo (R)
		Política de Sanciones (R)
		Revisión de la Actividad del Sistema de Información (R)
Responsabilidad de seguridad asignada	164.308(a)(2)	(R)
Seguridad de la fuerza de trabajo	164.308(a)(3)	Autorización y/o Supervisión (D)
		Procedimiento de autorización de mano de obra (D)
		Procedimiento de Terminación (D)
Gestión de Acceso a la Información	164.308(a)(4)	Aislar las funciones del centro de atención de salud (R)
		Autorización de Acceso (D)
		Establecimiento de Acceso y modificación (D)
Concientización y Capacitación de Seguridad	164.308(a)(5)	Recordatorios de Seguridad (D)
		Protección contra Software Malicioso (D)
		Monitoreo de inicio de sesión (D)
		Gestión de claves (D)
Procedimientos de Incidentes de Seguridad	164.308(a)(6)	Reporte y Respuesta (R)
Plan de Contingencia	164.308(a)(7)	Plan de Respaldo de Datos (R)
		Plan de Recuperación de Desastres (R)
		Plan de Operación en modo Emergencia (R)
		Procedimiento de Revisión y Pruebas (D)
		Análisis de Datos Críticos y Aplicaciones (D)
Evaluación	164.308(a)(7)	(R)
Contratos de Socios de Negocios y Otros Arreglos	164.308(b)(2)	Contrato Escrito u otro Arreglo (R)
Salvaguardas Físicas		
Control de Acceso a Instalaciones	164.310(a)(1)	Operaciones de Contingencia (D)
		Plan de Segurida de la Instalación (D)
		Procedimientos de Control de Acceso y Validación (D)
		Registros de Mantenimiento (D)
Uso de la Estación de Trabajo	164.310(b)	(R)
Seguridad de la Estación de Trabajo	164.310(c)	(R)
Control de dispositivos y medios	164.310(d)(1)	Disposición (R)
		Reutilización de Medios (R)
		Trazabilidad (D)
		Almacenamiento y Respaldo de Datos (D)
Salvaguardas Técnicas		
Control de Acceso	§164.312(a)(1)	Identificador de usuario único (R)
		Procedimiento de acceso de emergencia (R)
		Desconexión automática (D)
		Cifrado y Descrifrado (A)
Controles de auditoria	§164.312(b)	(R)
Integridad	§164.312(c)(1)	Mecanismo para autenticar ePHI (A)
Autenticación de entidad o persona	§164.312(d)	(R)
Seguridad en la Transmisión	§164.312(e)(1)	Controles de Integridad (A)
		Cifrado (A)

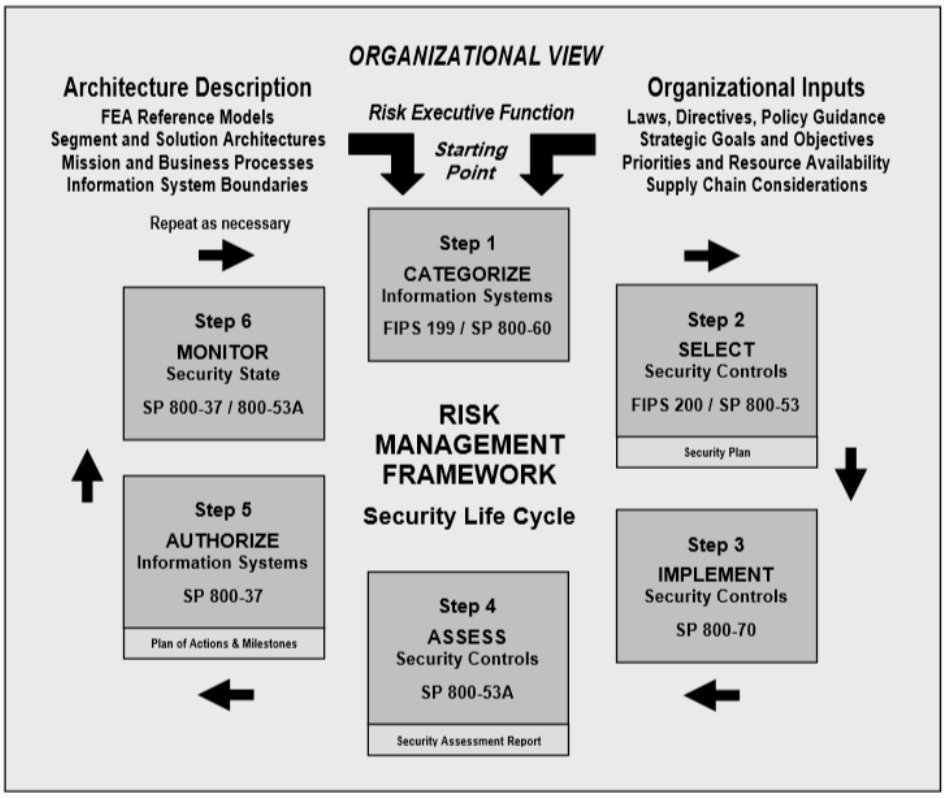
Fuente: [29]

Como se puede observar la regla de Seguridad de HIPAA requiere que las entidades cubiertas y los asociados de negocios lleven a cabo un análisis de riesgo e implementen salvaguardas técnicas, físicas y administrativas para la ePHI. La Oficina de Derechos Civiles (OCR) de HHS hace cumplir la Regla de Seguridad de HIPAA, la cual a su vez requiere que las entidades reguladas de HIPAA evalúen continuamente los riesgos de seguridad de sus procesos y sistemas. OCR en conjunto con la Oficina del Coordinador Nacional de Salud (ONC), genero una guía de evaluación de riesgos, para ayudar a las entidades cubiertas por la HIPAA a proteger la ePHI a través de salvaguardas técnicas. Las salvaguardas técnicas incluyen hardware, software y otras tecnologías que limitan el acceso al ePHI [30].

En octubre del 2008 el *National Institute of Standards and Technology* (NIST) realiza una publicación de seguridad *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* SP 800-66 donde resume las normas de seguridad de la HIPAA y explica la organización de la Regla de Seguridad. La publicación tiene como objetivo educar a los lectores acerca de los términos de seguridad de la información usados en la Regla de Seguridad de HIPAA e identifica actividades típicas que debe considerar una entidad cubierta para implementar un programa de seguridad de la información. La publicación SP 800-66 no complementa, reemplaza, modifica o reemplaza la propia Regla de Seguridad [27].

NIST también entrega un *framework* completo para el manejo de riesgo basado en un conjunto de publicaciones SP 800-series, estableciendo un proceso basado en riesgo para proteger la ePHI tal como se muestra en la figura de abajo, donde cada uno de los seis pasos de la gestión de riesgo NIST tiene un mapeo directo con la regla de seguridad HIPAA.

Figura 3.7NIST *Risk Management Framework*



Fuente: [27]

En la figura abajo se explica cada etapa y su mapeo con las directivas de la regla de seguridad.

Figura 3.8 Mapeo de NIST Risk Management Framework (RMF) y la regla de seguridad.

Etapa	Descripción	Mapeo a la regla de seguridad
Categorizar sistemas de información	Es el primer paso y emplea FIPS 199 y NIST SP 800-60 para determinar la criticidad y la sensibilidad del sistema de información y la información procesada, almacenada y transmitida.	Identificar activos y sistemas de información que generan, reciben, transmiten o mantengan ePHI. 164.308(a)(1)(i) – Security Management Process
Seleccionar controles de seguridad	Este paso emplea FIPS 200 y NIST SP 800-53 para identificar y especificar controles de seguridad apropiados para el sistema de información. La selección de los controles de seguridad para los procesos de misión / negocio de una organización y los sistemas de información que apoyan esos procesos. Es una actividad de mitigación de riesgos.	Seleccione los estándares y las especificaciones de implementación requeridas como el conjunto de control de seguridad inicial. Estos controles de seguridad requeridos establecen la línea de base desde la cual se evalúa el riesgo para ePHI. 164.308(a)(1)(i) – Security Management Process 164.308(a)(1)(ii)(A) – Risk Analysis 164.308(a)(1)(ii)(B) – Risk Management 164.316(b)(1) – Documentation 164.316(b)(2)(ii) – Updates
Implementar controles de seguridad	Emplea arquitecturas empresariales, el Ciclo de Vida del Desarrollo de Sistemas (SDLC) y varias publicaciones del NIST para guiar la implementación de controles de seguridad en sistemas de información organizacional.	Implementar los controles de seguridad que se han determinado razonables y apropiados para la organización. 164.308(a)(1)(ii)(B) – Risk Management
Evaluar los controles de seguridad	emplea NIST SP 800-53A para evaluar los controles de seguridad del sistema de información.	Evaluar las especificaciones implementadas. 164.308(a)(8) – Evaluation
Autorizar sistema de información	Autorizar el funcionamiento del sistema de información (con controles de seguridad implementados) basado en la determinación del riesgo para las operaciones organizacionales, los activos de la organización, los individuos y otras organizaciones, y una decisión explícita de aceptar este riesgo.	Inherente a cualquier proceso de gestión de riesgos es la aceptación de aquellos riesgos identificados que se consideran aceptables para la organización. 164.308(a)(1)(ii)(B) – Risk Management
Monitorear el estado de la seguridad	Supervisar y evaluar de forma continua los controles de seguridad seleccionados en el sistema de información.	Una entidad cubierta debe revisar y actualizar periódicamente sus medidas de seguridad y docum.entación. 164.308(a)(8) – Evaluation 164.308(a)(1)(ii)(D) – Information System Activity Review

Fuente: Elaboración propia

3.3.3 Salvaguardas técnicas de la regla de seguridad

Se va a dedicar una sección para explicar los requerimientos técnicos de la regla de seguridad HIPAA, por ser los que apliquen directamente sobre la cadena de bloques. Esto no quiere decir que no cumple las otras reglas, solo que son aplicables al entorno de uso de la cadena de bloques. Por ejemplo, las salvaguardas administrativas aplican al personal que use la solución y la gestión de los sistemas que generan, mantienen y transmiten la ePHI.

La Regla de Seguridad define salvaguardas técnicas en el apartado 164.304 como "la tecnología, la política y los procedimientos que protegen la ePHI y controlan su acceso" [26].

La Regla de Seguridad se basa en los conceptos fundamentales de flexibilidad, escalabilidad y neutralidad tecnológica. Por tanto, permite que una

entidad cubierta utilice cualquier medida de seguridad que le permita implementar apropiadamente las normas. Las salvaguardas técnicas definen cinco normas que deben implementarse: Control de acceso, controles de auditoria, Integridad, Autenticación de entidad o persona y Seguridad en la transmisión. En la figura se observa la matriz de especificaciones y a continuación su descripción.

Figura 3.9 Seguridades Técnicas de la regla de Seguridad

Salvaguardas Técnicas			
Estándares	Secciones	Especificaciones de implementación (R)=Requerido, (D)= Deseable	
Control de Acceso	§164.312(a)(1)	Identificador de usuario único	(R)
		Procedimiento de acceso de emergencia	(R)
		Desconexión automática	(D)
		Cifrado y Descrifrado	(D)
Controles de auditoria	§164.312(b)		
Integridad	§164.312(c)(1)	Mecanismo para autenticar ePHI	(D)
Autenticación de entidad o persona	§164.312(d)		
Seguridad en la Transmisión	§164.312(e)(1)	Controles de Integridad	(D)
		Cifrado	(D)

Fuente: [26]

a) Control de acceso. La Regla de Seguridad define el acceso en la sección 164.304 como "la habilidad o los medios necesarios para leer, escribir, modificar o comunicar datos / información o usar cualquier recurso del sistema" [26]. Los controles de acceso proveen a los usuarios los privilegios para ingresar y realizar funciones sobre los sistemas de información, aplicaciones, programas o archivos. En otras palabras, los controles de acceso habilitan a los usuarios acceder al mínimo necesario de información necesitado para rendir sus funciones laborales.

   Los derechos o privilegios deben ser otorgados a los usuarios autorizados basado en perfiles de acceso que la entidad cubierta debe haber implementado como parte de las salvaguardas administrativas 164.308(a)(4) que describe el estándar para la gestión del acceso a la información. Para cumplir con la norma se deben implementar cuatro especificaciones técnicas: Identificación única de usuario, Procedimiento de acceso de emergencia,

Desconexión automática, y cifrado descifrado de datos. En la siguiente figura se describirá las especificaciones del control de acceso.

Figura 3.10 Control de Acceso y sus especificaciones.

Control de acceso	
Especificación de la norma	Descripción
Identificación única de usuario (Requerida)	La Identificación única de usuario permite a una entidad realizar un seguimiento de la actividad específica de cada usuario cuando está conectado a un sistema de información. Así, se pueden asignar responsabilidades de las funciones que se realizan en los sistemas de información con ePHI cuando los usuarios se conectan a dichos sistemas.
Procedimiento de acceso de emergencia (Requerida)	El procedimiento de acceso de emergencia son instrucciones documentadas y prácticas operativas para obtener acceso a la ePHI necesaria durante una situación de emergencia. Los controles de acceso son necesarios en condiciones de emergencia, aunque pueden ser muy diferentes de los utilizados en circunstancias de operación normal.
Desconexión automática (Deseable)	La desconexión automática es una forma efectiva de impedir que usuarios no autorizados accedan a ePHI en una estación de trabajo cuando se deja sin atención durante un período de tiempo. Después de un período predeterminado de inactividad, la aplicación automáticamente desconectará al usuario.
Cifrado y descifrado	Si la información está cifrada, habría una baja probabilidad de que cualquier persona que no sea la parte receptora sea capaz de descifrar el texto. El objetivo del cifrado es proteger a EPHI de ser accedida por usuarios no autorizados.

Fuente: Elaboración propia

b) Controles de Auditoria. La norma cita “Implementar hardware, software, mecanismos o procedimientos que registran y examinan la actividad en sistemas de información que contienen o usan información de ePHI” [26]. Es importante señalar que la Regla de Seguridad no identifica los datos que deben ser recopilados por los controles de auditoría ni la frecuencia con la que deben revisarse los informes de auditoría. Una entidad cubierta debe realizar un análisis de riesgos de sus recursos organizacionales, tales como la infraestructura técnica, las capacidades de seguridad de hardware y software, para determinar los controles de auditoría apropiados para los sistemas de información que contienen o usan ePHI.
c) Controles de integridad. La norma la define como "La propiedad de que los datos o la información no hayan sido alterados o destruidos de manera no autorizada" [26]. La norma de integridad requiere que se implementen políticas y procedimientos para proteger la ePHI de su alteración o destrucción. Esta norma solo contiene una especificación deseable: Mecanismo para autenticar ePHI que requiere “Implementar mecanismos electrónicos para corroborar

que la ePHI no ha sido alterada o destruida de manera no autorizada" [26].

d) Autenticación de entidad o persona. Especifica implementar procedimientos para verificar que una persona o entidad que requiere acceso a la ePHI es quien dice ser.
e) Seguridad en la transmisión. La norma requiere implementar medidas técnicas de seguridad para prevenir el acceso no autorizado a ePHI que se está transmitiendo a través de una red de telecomunicaciones. Consta de dos especificaciones técnicas deseables que se describen en la siguiente figura.

Figura 3.11 Seguridad en la transmisión y sus especificaciones

Seguridad en la transmisión	
Especificación de la norma	Descripción
Controles de Integridad (Deseable)	Implementar medidas de seguridad para asegurar que la ePHI transmitida sobre una red de telecomunicaciones no se modifique indebidamente sin detección hasta que sea entregada a su receptor.
Cifrado (Deseable)	Implementar un mecanismo para cifrar ePHI cuando se transmite a sobre una red de telecomunicaciones.

Fuente: Elaboración propia.

3.4 Enfoque de la Cadena de Bloques como una solución.

La Ley de Protección al Paciente y Asistencia Asequible de 2010 creó el Fondo Fiduciario de Investigación de Resultados Centrados en el Paciente o *Patient-Centered Outcomes Research Trust Fund* (PCORTF) para ayudar a construir la capacidad nacional y la infraestructura necesarias para llevar a cabo la investigación de resultados centrada en el paciente o *Patient-Centered Outcomes Research* (PCOR). El objetivo final de estos esfuerzos es permitir que los pacientes y entidades cubiertas tomen decisiones de salud más informadas. El secretario del HHS delegó la autoridad en la Oficina del Subsecretario de Planificación y Evaluación u *Office of The Assistant Secretary for Planning and Evaluation* (ASPE) para coordinar e implementar un plan estratégico que invierta estos fondos de manera efectiva.

La Ley de Reautorización de América *Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science* (COMPETES) [31], aprobada en diciembre de 2010, permite a cualquier jefe

de la agencia "llevar a cabo un programa para conceder premios competitivos para estimular la innovación" Desde entonces, la Oficina Nacional de Coordinación u *Office of the National Coordinator* (ONC) comenzó a hacer frente a desafíos en 2011 bajo esta ley.

Los retos permiten al público resolver los problemas presentados por la ONC y recibir premios por las mejores soluciones. En el nivel más básico, los retos contienen tres pasos: primero ONC anuncia un problema al público; segundo los participantes crean y presentan soluciones al problema; por último, ONC evalúa esas soluciones y premia a los mejores.

El 6 de julio del 2016 se anunció el reto "Uso de la Cadena de Bloques en la salud IT y la investigación relacionada con la salud" [32], donde se solicitó examinar cómo el uso de la Cadena de Bloques podía promover las necesidades de interoperabilidad de la industria expresadas en el *Shared Nationwide Interoperability Roadmap* [33] del ONC, PCOR, *Precision Medicine Initiative* (PMI).

La ONC recibió 70 propuestas del público, de las cuales se seleccionaron 15 opciones ganadoras en agosto 29 del 2016 [32]. Y se seleccionaron 8 *white papers* que se expusieron en el Taller de investigación en las oficinas principales de NIST el 26 y 27 de septiembre del 2016 [34], de los cuales vamos a explicar algunos a continuación.

Blockchain: The Chain of Trust and its Potential to Transform Healthcare – IBM's Point of View [34]

En el reporte el equipo de IBM describe los beneficios de la cadena de bloques, se basan en las capacidades de la misma para elaborar una tabla de potenciales usos de la cadena de bloques en desafíos de la salud. Además, no proponen una implementación de facto, sino que hacen referencia a la tecnología como tal, cabe destacar que IBM tiene su propia solución llamada *Hyperledger* [35]. No se va a explicar el *white paper* debido a que no presenta una propuesta de implementación para explicar.

Blockchain: Securing a New Health Interoperability Experience

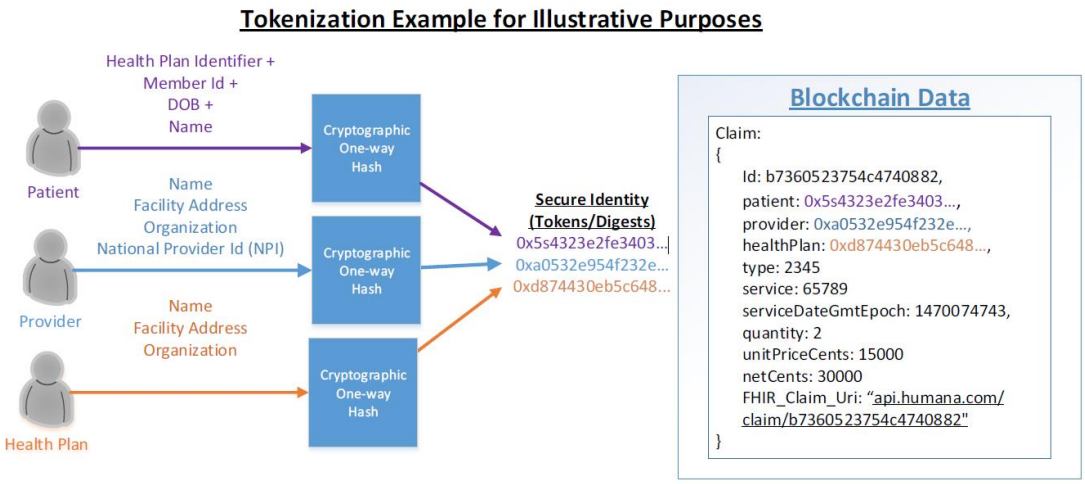
Es un reporte de Accenture de como la cadena de bloques puede apoyar al campo de la salud, tampoco ofrecen una implementación para explicar en detalle. La conclusión de Accenture respecto al uso de la cadena de bloques es apoyo al paciente y los proveedores de salud, para citarlos "los pacientes se dan cuenta del valor de sus datos de salud y son compartidos de forma segura como parte de un sistema de atención de salud en constante aprendizaje"; y "los proveedores aprovechan los datos sanitarios para mejorar la salud y el bienestar de sus pacientes con mejores resultados clínicos y financieros" [34].

Blockchain Technologies: A discussion on how the claims process can be improved

El reporte realizado por Culver entrega una solución basada en contratos inteligentes para agilizar el proceso de costeo de la atención sanitaria, construyendo una plataforma interoperable, transparente y exacta. De esta manera, ahorra tiempo y esfuerzo en el proceso de reclamaciones actual ante los seguros de salud.

La solución contempla codificar en un contrato inteligente la relación entre los proveedores de salud, los pacientes y los seguros médicos. De tal forma que en la cadena de bloques solo se almacene una *Uniform Resource Locator* (URL) hacia un reclamo del seguro por una atención. Solo almacena la URL para disminuir la cantidad de datos que almacena la cadena y mantiene la privacidad del paciente integrando un hash con datos propios, tal como se muestra en la figura abajo.

Figura 3.12 Ejemplo de un token utilizado en la cadena de bloques

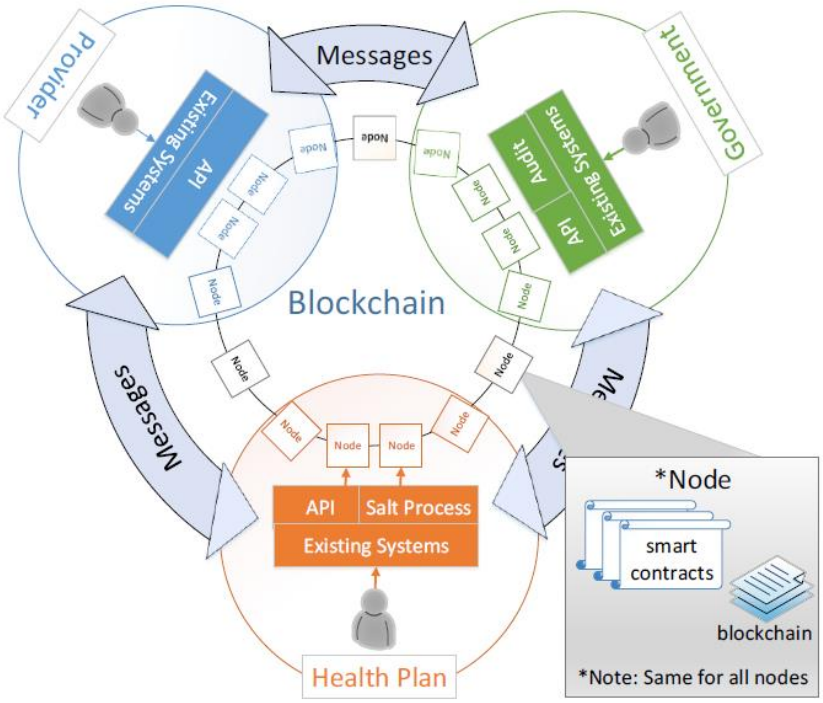


Fuente: [34]

Mantiene los datos del tipo, servicio, *timestamp* y costo en texto claro para que pueda ser ejecutado por el contrato inteligente cargado en la cadena de bloques de tal forma que pueda acumular los costos por el plan de salud o empresa de seguros que cubre al paciente.

La arquitectura propone integrar la cadena de bloques por los Proveedores de salud, los Planes de salud y el Gobierno. En consecuencia, será una cadena de bloques privada como se muestra en la figura.

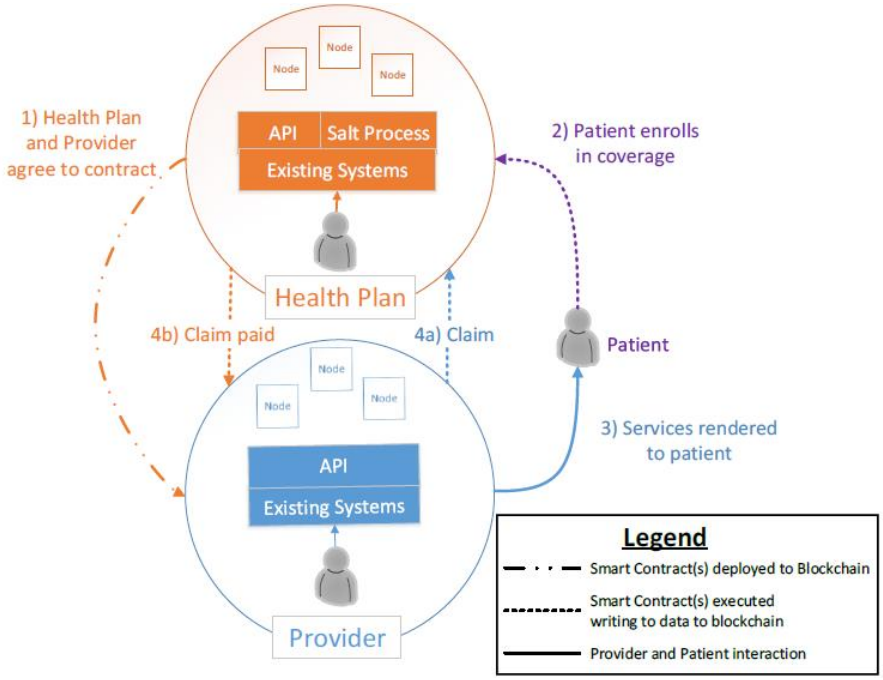
Figura 3.13 Arquitectura de la solución Culver



Fuente: [34]

Un posible flujo de funcionamiento de la cadena podría ser:

Figura 3.14 Flujo de funcionamiento de solución Culver



Fuente: [34]

a) El plan de salud o aseguradora y el proveedor de salud acuerdan un contrato de provisión de servicios. En este paso se carga un contrato inteligente con cláusulas y costos asociados entre las entidades.

b) El paciente se enrola en un plan de salud o cobertura de seguro de salud. Aquí se ejecuta una instancia del contrato inteligente con los datos del paciente y una cobertura. El ejecutor es el Plan de salud ya que el paciente no es parte de la cadena.

c) El Paciente interactúa con un proveedor de salud por atención médica. El Proveedor validará la cobertura en la cadena de bloques porque tendrá el *token* de enrolamiento generado en el primer paso y atenderá al paciente.

d) El Proveedor de salud generará el reclamo respectivo contra el Plan de salud ejecutando el contrato con el token el Paciente y la información respectiva.

e) El Plan de salud así mismo validará y responderá al pago del reclamo del Proveedor de salud.

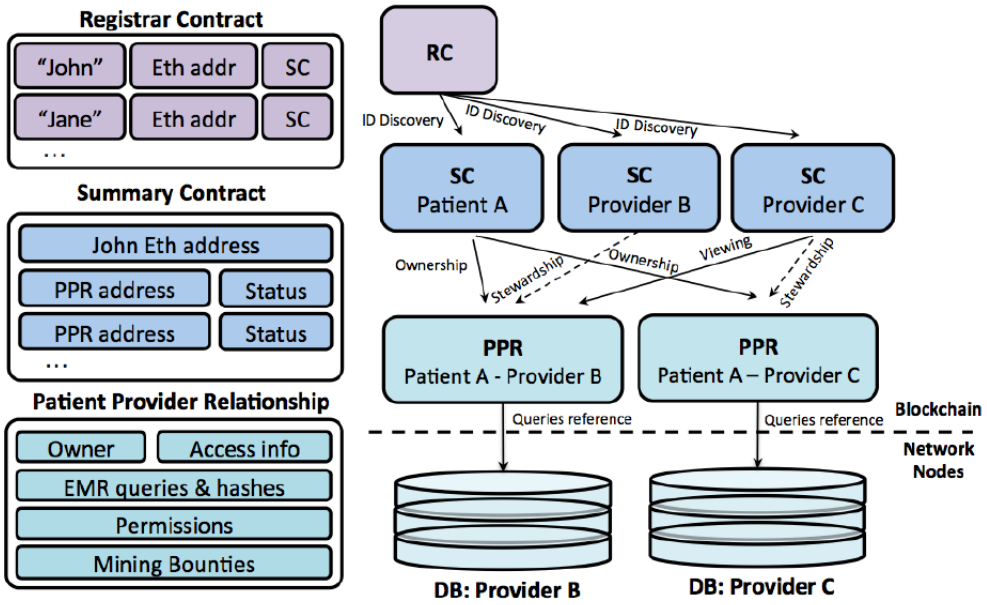
"MedRec" Using Blockchain for Medical Data Access and Permission Management

Este reporte propone MedRec, una solución que gestiona la autenticación, confidencialidad, trazabilidad y el intercambio de datos en un diseño modular que se integra con las soluciones existentes de almacenamiento de datos locales de los proveedores, facilitando la interoperabilidad y adaptabilidad. La implementación de Cadena de bloques MedRec aborda cuatro problemas de las EHR: acceso fragmentado y lento a la información de EHR, interoperabilidad del sistema, la gestión de datos de pacientes y mejorar la investigación médica en cuanto a calidad y cantidad de datos.

MedRec usa como base 3 tipos de contratos inteligentes sobre Ethereum: *Registrar Contract* (RC), *Patient-Provider Relationship Contract* (PPR) y *Summary Contract* (SC).

Los contratos se hacen para contener metadatos sobre la propiedad del registro, los permisos y la integridad de los datos. Las transacciones de la cadena de bloques en MedRec llevan instrucciones criptográficamente firmadas para administrar estas propiedades. Como se muestra en la figura abajo.

Figura 3.15 Contratos inteligentes usados en la implementación MedRec y su relación.



Fuente: [34]

El contrato global RC mapea las cadenas de identificación de los participantes a sus respectivas direcciones Ethereum o clave pública. Las políticas programadas en el contrato regulan el registro de nuevas identidades o el cambio de mapeos. Por tanto, se puede restringir el registro de identidades solo a entidades certificadas o proveedores de salud. Además, también mapea la dirección de un contrato especial llamado SC.

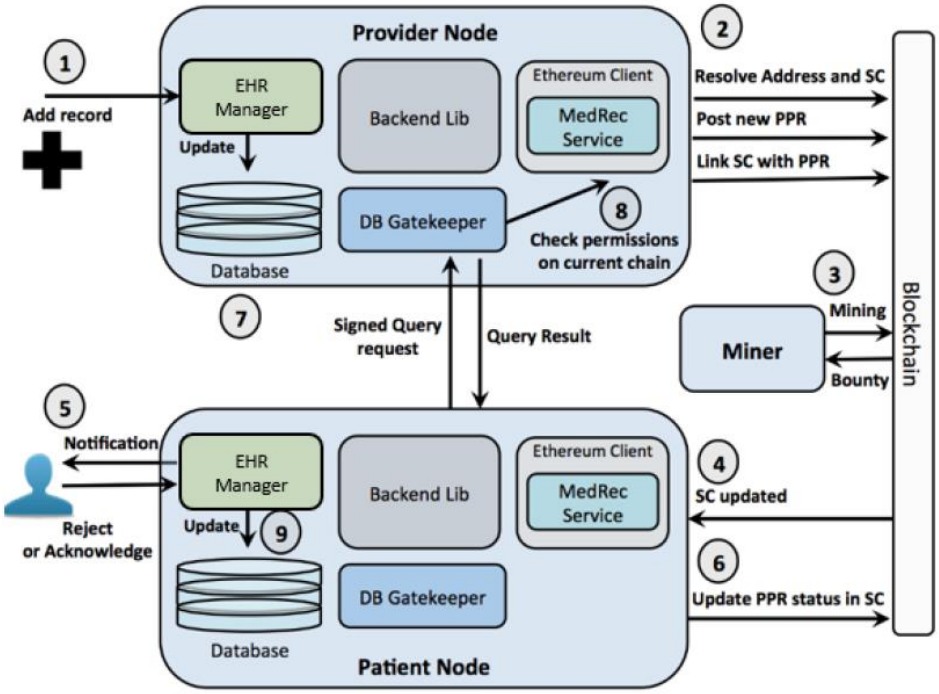
Un PPR es un contrato emitido entre dos nodos en el sistema. Cuando un nodo almacena y administra EHR para otro nodo. El PPR tiene información acerca del proveedor de servicios, permisos de acceso, enlace de consulta del EHR, *hashes* y regalías por minería.

El SC es un contrato que contiene una lista de referencia a los contratos PPR para los participantes en el sistema para localizar su lista de EHR que conforman su HCE. Desde el punto de vista del paciente su SC tendría toda

su HCE o interacciones con los proveedores de salud que lo han atendido. Desde el punto de vista del proveedor de salud el SC contiene la lista de todos los pacientes que han atendido y la lista de terceras partes que han sido autorizados por los pacientes para acceder a los respectivos EHR.

La arquitectura del sistema como se muestra en la figura inferior consta de una cadena de bloques donde participan pacientes y proveedores de servicios de salud.

Figura 3.16 Arquitectura de solución MedRec



Fuente: [34]

Un nodo esta consta de 4 componentes de software: un cliente Ethereum, librería de *Backend*, DB *Gatekeeper* y un EHR *Manager.*

En la figura se pueden ver las diferencias entre los nodos y sus acciones: el nodo proveedor puede insertar EHR y el nodo Paciente puede recibir notificaciones y aceptar o denegar peticiones. Para ilustrar el funcionamiento de la cadena revisaremos paso a paso su funcionamiento:

1) El proveedor adiciona un EHR para un nuevo paciente, esto acciona el EHR Manager que grabará el registro localmente en el sistema propietario del cliente y al mismo tiempo será enviado a la librería

de Backend. La librería realiza una abstracción del manejo del cliente Ethereum y sus funciones para construir bloques como contratos inteligentes.

2) El cliente Ethereum va a realizar los siguientes pasos: usando la información del paciente y el contrato RC sobre la cadena, se obtendrá la dirección Ethereum del paciente y su correspondiente contrato SC. A continuación, el proveedor enviará un PPR a la cadena, indicando la administración sobre la información propiedad del paciente que corresponde a la dirección Ethereum que fue recuperada. Además, el nodo proveedor construye un enlace de consulta para hacer referencia a los datos y actualiza el PPR. Finalmente, el nodo proveedor envía una transacción que vincula el nuevo PPR al SC del paciente, para permitir que el nodo paciente ubique la información de ese evento posteriormente en la cadena de bloques.
3) La transacción PPR vinculada al SC del paciente es minada por cualquier nodo en la red.
4) El cliente Ethereum del paciente monitorea continuamente su SC. En el paso 3 se minó la transacción que añade un PPR al SC del paciente, por lo cual el monitoreo envía una notificación al paciente.
5) El paciente puede aceptar o rechazar la interacción con el proveedor.
6) El paciente al interactuar con la notificación lo que hace es modificar una variable de estatus privada y actualiza el SC. Enviando una transacción a la cadena con la actualización del SC.
7) En caso de que el paciente aceptará el PPR, el nodo paciente emite una consulta de la información cargada por el proveedor usando el link de consulta y firmando criptográficamente la petición.
8) El gatekeeper confirma la identidad del emisor de la petición y usando la dirección ethereum del emisor confirma su acceso. Por último, realiza su consulta sobre el EHR Manager y da como respuesta el EHR.
9) El nodo paciente actualiza su base local con la respuesta del paso anterior.

Conclusiones

Después de una revisión total de Bitcoin y sus conceptos se puede llegar a la conclusión que la criptomoneda es una aplicación de la cadena de bloques, aunque cuando se creó nació como Bitcoin [36].

La cadena de bloques es una tecnología que reúne varios protocolos que funcionan en sincronía para lograr una solución eficiente en el tiempo garantizando características claves como el anonimato basado en la criptografía asimétrica, la integridad lograda con el encadenamiento hacia atrás más el hashing y la prueba de trabajo, la disponibilidad ante su tolerancia a fallas sustentada por su red par a par. Si bien la cadena expuesta por Bitcoin fue diseñada para cargar valores pequeños en las transacciones, lo cual ayuda a hacer el bloque ligero en tamaño, procesamiento y replicación; pero, restringe las distintas soluciones que se pueden cargar sobre el bloque a únicamente criptomonedas. Sin embargo, esto abre las posibilidades de investigación para crear cadenas laterales o base de datos distribuidas que pueda contener grandes volúmenes de información.

Se debe establecer un marco ante el cual decidir usar una cadena de bloques pura o una programable, si bien su versión nativa tiene un conjunto básico de operaciones limitadas a la criptomoneda con unos pocos ajustes se puede lograr guardar hashes de información que resida en otro lugar. Ahora su versión programable ofrece muchos beneficios para establecer reglas y que se vayan ejecutando sin la intervención del usuario, pero deja la observación de tener código poco fiable corriendo en todos los nodos de la red cargado por usuarios de la cadena.

Revisando la problemática de las historias clínicas electrónicas desde sus inicios hasta los últimos años y dando una vista general de los requerimientos de seguridad que exige el almacenamiento de este tipo de información, se puede concluir que la cadena de bloques puede ser una excelente solución para este tipo de aplicaciones. Es claro que todavía quedan problemas por solucionar como la entrega o generación de llaves al paciente, el lugar donde residirá toda la información, el incentivo para el minado de los bloques, el tipo de cadena de bloques privada o pública, los

permisos de acceso a la información, los derechos de propiedad sobre la información, la cantidad de información a subir a la cadena, los posibles orígenes de información autorizados para subir información.

Al validar la matriz de reglas de seguridad del HIPAA, en particular las especificaciones para implementar las salvaguardas técnicas podemos concluir que cumplimos con todas las normas requeridas y deseables. Pero hay puntos importantes para resolver que se muestran en la tabla inferior.

Tabla 1. Especificaciones Técnicas de la regla de seguridad versus la Cadena de Bloques.

Norma	Especificación para implementación	Cadena de bloques
Control de Acceso	Identificación única de usuario (Requerida)	Cada usuario puede tener una identificación única dentro de la cadena de bloques. Inclusive puede ser más de una. Las identificaciones están ligadas a las llaves privadas y públicas que puede generar un usuario. Aquí existen algunos temas para analizar: - Se deberá asignar las llaves por parte de un ente central como el gobierno o ministerio de salud o se permitirá al usuario generar sus propias llaves. - El gobierno tendrá acceso al mapeo identificación nacional de usuario contra su llave pública. Para todos estos casos va a afectar la privacidad del usuario, ya que existirá un ente que puede mapear usuario con ePHI. Sin embargo, se cumplirá con el estándar.
	Procedimiento de acceso de emergencia (Requerida)	Este tipo de procedimientos puede ocasionar problemas de seguridad, pero es obligatorio para el cumplimiento de la norma. En todo caso, siempre debe existir una forma de acceso a la información por emergencia sea por perdida de las claves por parte del usuario o por parte de la entidad cubierta que resulta en la denegación de acceso a la información. En la cadena de bloques se debe analizar un esquema multifirma que permita el acceso a la información al usuario y la entidad cubierta que la genero.

Control de Acceso	Desconexión automática (Deseable)	Cumple sin problemas. No hay temas para analizar.
	Cifrado y descifrado (Deseable)	Cumple sin problemas. Toda información independientemente de donde se almacene puede guardarse cifrada con la clave del usuario y una clave especial de la entidad cubierta que genero la información en un esquema multifirma.
Controles de Auditoria	Esta especificación se debe analizar en el sistema cliente que se conecta a la cadena de bloques, una analogía del monedero de Bitcoin que genera las transacciones, en este caso se generan EHR para su inserción en la cadena de bloques. Una solución es permitir que solo las entidades cubiertas puedan generar transacciones, pero se debe contemplar una cadena de bloques en paralelo que mantenga un registro o log de actividades y el usuario que la generó.	
Controles de integridad	Mecanismo para autenticar ePHI (Deseable)	La cadena de bloques cumple esta especificación por defecto con sus especificaciones de encadenamiento hacia atrás en el tiempo y árbol de Merkle que permite comprobar que un dato es parte de un bloque.
Autenticación de entidad o persona	La especificación se cumple con la clave privada del individuo para visualizar la ePHI y la clave privada de la entidad cubierta que puede agregar datos. Sin embargo, la gestión de las claves puede ser un tema de riesgo debido a los trabajadores de las entidades cubiertas y el esquema de cuidado de las claves de los individuos.	
Seguridad en la transmisión	Controles de Integridad (Deseable)	Una de las soluciones es mantener una base cifrada distribuida entre los proveedores de salud. Manteniendo en la cadena de bloques el hash de cada registro almacenado en dicha base, de tal forma que se guarda la integridad de cada dato. Sin embargo, está técnica solo sirve para datos almacenados, un dato recién generado debe ser cifrado antes de enviarlo a la base distribuida y calculado su hash antes de ser incluido en un bloque para minar. Este punto debe ser analizado en más detalle solo en la creación del registro.
	Cifrado (Deseable)	

Fuente: Elaboración propia.

Revisando varios reportes de uso de la cadena de bloques para la protección de datos privados y registros médicos da como resultado varias mezclas de Ethereum con Bases de datos locales, lo cual soluciona parte del problema, pero abre más interrogantes como la fiabilidad del ente que albergará la base de datos, las posibles fallas de código en Ethereum originando autorizaciones indebidas para la lectura de información. Estos primeros avances servirán para iniciar nuestro siguiente trabajo y plantear el diseño de un sistema completo para el manejo de historias clínicas electrónicas.

Bibliografía

[1] E. Kiktenko, N. Pozhar, M. Anufriev, A. Trushechkin, R. Yunusov, Y. Kurochkin, A. Lvovsky y A. Fedorov, «Quantum-secured blockchain,» Russian Quantum Center, Moscu, 2017.

[2] Bitcoin, «Bitcoin,» Bitcoin, [En línea]. Disponible: https://bitcoin.org/es/descargar. [Último acceso: 27 04 2017].

[3] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [En línea]. Disponible: www.bitcoin.org. [Último acceso: 12 Octubre 2016].

[4] C. Corp, «STANDARDS FOR EFFICIENT CRYPTOGRAPHY,» Certicom Corp, 20 septiembre 2000. [En línea]. Disponible: http://www.secg.org/SEC2-Ver-1.0.pdf. [Último acceso: 7 mayo 2017].

[5] BitcoinWiki, «Bitcoin IT - Base58Check,» Bitcoin, 24 octubre 2016. [En línea]. Disponible: https://es.bitcoin.it/wiki/Codificaci%C3%B3n_Base58Check. [Último acceso: 7 mayo 2017].

[6] M. A. Andreas, Mastering Bitcoin, Sebastopol, CA: O'Reilly, 2014.

[7] P. Wuille, «GitHub BIP0032,» 11 febrero 2012. [En línea]. Disponible: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki. [Último acceso: 8 mayo 2017].

[8] A. Narayanan, J. Boneau, E. Felten, A. Miller y S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton: Princeton University Press, 2016.

[9] Bitcoin, «Bitcoin nodes,» Bitcoin community, 10 febrero 2017. [En línea]. Disponible: https://github.com/bitcoin/bitcoin/blob/master/contrib/seeds/nodes_main.txt. [Último acceso: 27 mayo 2017].

[10] Bitcoin, «Bitcoin DNS seeder,» 13 enero 2017. [En línea]. Disponible: https://github.com/sipa/bitcoin-seeder. [Último acceso: 27 mayo 2017].

[11] M. Hearn y M. Corallo, «Github BIP0037,» Bitcoin, 24 octubre 2012. [En línea]. Disponible: https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki. [Último acceso: 27 abril 2017].

[12] S. Brakeville y B. Perepa, «IBM developerWorks,» IBM, 9 mayo 2016. [En línea]. Disponible: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/. [Último acceso: 29 mayo 2017].

[13] Ethereum, «GitHub Ethereum,» 5 enero 2017. [En línea]. Disponible: Patricia Tree. [Último acceso: 05 junio 2017].

[14] G. Greenspan, «Multichain,» Coin Sciences Ltd., julio 2015. [En línea]. Disponible: http://www.multichain.com/download/MultiChain-White-Paper.pdf. [Último acceso: 05 junio 2017].

[15] Hessiod Services LLC, «Bitcoin Mining,» Hessiod Services LLC, [En línea]. Disponible: https://www.bitcoinmining.com/what-is-proof-of-work/. [Último acceso: 28 mayo 2017].

[16] J. Halamka, A. Lippman y A. Ekblaw, «The Potential for Blockchain to Transform Electronic Health Records,» 3 marzo 2017. [En línea]. Disponible: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records. [Último acceso: 28 mayo 2017].

[17] M. Pease, R. Shostak y L. Lamport, «Reaching Agreement in the Presence of Faults,» *Journal of the ACM,* vol. 27 Issue 2, nº 0004-5411 , pp. 228-234, 4 abril 1980.

[18] International Organization for Standardization, «Health informatics — Electronic health record — Definition, scope and context,» octubre 2005. [En línea]. Disponible: https://www.iso.org/obp/ui/#iso:std:iso:tr:20514:ed-1:v1:en:en. [Último acceso: 15 junio 2017].

[19] T. Gunter y N. Terry, «The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions,» *Journal of Medical Internet Research,* vol. 7, nº 1, 14 marzo 2005.

[20] D. Luna, E. Soriano y F. Gonzalez, «Revista del Hospital Italiano,» diciembre 2007. [En línea]. Disponible: https://www.hospitalitaliano.org.ar/multimedia/archivos/servicios_attachs/5056.pdf. [Último acceso: 14 junio 2017].

[21] D. Luna, E. Soriano y F. González, «Historia clínica electrónica,» diciembre 2007. [En línea]. Disponible: http://revista.hospitalitaliano.org.ar. [Último acceso: 11 mayo 2017].

[22] National Academy of Sciences, For the Record: Protecting Electronic Health Information, Washington D.C.: National Academy Press, 1997.

[23] Committee on Data Standards for Patient Safety, «Key Capabilities of an Electronic Health Record System,» National Academies Press, Washington D.C., 2003.

[24] J. H. University, «Hippocratic Oath,» The Sheridan Libraries, 14 abril 2017. [En línea]. Disponible: http://guides.library.jhu.edu/bioethics . [Último acceso: 18 junio 2017].

[25] R. Gelpi, M. Perez, A. Rancich y J. Mainetti, «Confidencialidad en los Juramentos Medicos,» *Medicina Buenos Aires,* vol. 60, nº 4, 2000.

[26] U.S. Department of Health & Human Services , «Health Insurance Portability and Accountability Act of 1996,» 21 agosto 1996. [En línea]. Disponible: https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996. [Último acceso: 16 septiembre 2017].

[27] National Institute of Standards and Technology, «An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,» octubre 2008. [En línea]. Disponible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf. [Último acceso: 18 septiembre 2017].

[28] U.S. Department of Health & Human Services, «Covered Entities and Business Associates,» 28 diciembre 2000. [En línea]. Disponible: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. [Último acceso: 16 septiembre 2017].

[29] DEPARTMENT OF HEALTH AND HUMAN SERVICES , «Health and Human Services,» 20 febrero 2003. [En línea]. Disponible: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es. [Último acceso: 17 septiembre 2017].

[30] ONC, «Security Risk Assessment Tool,» 13 marzo 2017. [En línea]. Disponible: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool. [Último acceso: 17 septiembre 2017].

[31] United States of America, «CONGRESS.GOV,» diciembre 2010. [En línea]. Disponible: https://www.congress.gov. [Último acceso: 23 septiembre 2017].

[32] Office of the National Coordinator , «Blockchain Challenge,» Innovation Center, 7 julio 2016. [En línea]. Disponible: http://www.cccinnovationcenter.com/challenges/block-chain-challenge/. [Último acceso: 23 septiembre 2017].

[33] Office of the National Coordinator for Health IT, «Shared Nationwide Interoperability Roadmap,» 2015. [En línea]. Disponible: https://www.healthit.gov/sites/default/files/hie-

interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. [Último acceso: 23 septiembre 2017].

[34] ONC Tech Lab Innovation, «Use of Blockchain in Healthcare and Research Workshop,» ONC Tech Lab Innovation, 7 septiembre 2016. [En línea]. Disponible: https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Use+of+Blockchain+in+Healthcare+and+Research+Workshop. [Último acceso: 30 septiembre 2017].

[35] The Linux Foundation, «HYPERLEDGER,» The Linux Foundation, [En línea]. Disponible: https://www.hyperledger.org/. [Último acceso: 30 septiembre 2017].

[36] D. Fernández, «Características criptográficas y potenciales debilidades de la criptodivisa Bitcoin,» Universidad de Buenos Aires, Buenos Aires, 2015.

[37] G. Zyskind, O. Nathan y A. Pentland, «Decentralizing Privacy: Using Blockchain to Protect,» de *2015 IEEE CS Security and Privacy Workshops*, Washington D.C., 2015.

[38] A. Ekblaw, A. Azaria, J. Halamka y A. Lippman, «A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data,» MIT Media Lab, Massachusetts, 2016.

[39] Blockchain Luxembourg S.A., «BLOCKCHAIN INFO,» Blockchain Luxembourg S.A., [En línea]. Disponible: https://blockchain.info/. [Último acceso: 28 junio 2017].

Tabla de Figuras