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

Carrera de Especialización en Seguridad Informática

Trabajo Final de la Especialización

Criptografía
Criptodivisas-Cryptocurrency

Características criptográficas y potenciales debilidades de la criptodivisa Bitcoin

Autora:
Diana Georgina Fernández Sánchez

Tutor del Trabajo Final:
Hugo Scolnik

2015
Cohorte 2014

Declaración Jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y 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”.

_____

Diana Georgina Fernández Sánchez

DNI: 95303923

Resumen

La presente investigación recopila información referente a la criptodivisa Bitcoin, desde sus características, elementos, funcionamiento y fundamentos criptográficos hasta las implicaciones de seguridad asociadas con su uso según los recientes análisis realizados por académicos alrededor del mundo, medios especializados y colaboradores/desarrolladores del protocolo de esta criptomoneda. Se inicia con un estudio previo de las bases que forman este protocolo, con énfasis en sus justificantes criptográficas y características de seguridad, para luego contrastar estos datos con las vulnerabilidades encontradas hasta el momento, con el fin de concluir sobre el panorama real de la tendencia Bitcoin en la sociedad actual.

Si bien esta investigación no demostró o refutó ninguna característica del protocolo (privacidad, eficiencia, trazabilidad, etc.) ni demostró en profundidad ningún ataque o vulnerabilidad del mismo, recopila una pequeña guía de lo que se puede esperar al utilizar esta tecnología: un sistema que si bien no es perfecto, si se toman las medidas necesarias de seguridad, puede resultar beneficioso para el usuario.

Palabras claves: criptomonedas, Bitcoin, delitos financieros, vulnerabilidades.

Índice General

Declaración Jurada de origen de los contenidos ..... **i**
Resumen ..... **ii**
Índice General ..... **iii**
Índice de tablas y figuras ..... **iv**
Agradecimientos ..... **v**
Nómina de abreviaturas ..... **vi**
Introducción **1**
Capítulo 1: Estado del arte de las criptodivisas **2**
1.1. Definición criptodivisa, tipos y ejemplos 2
1.2. Estado actual 3
Capítulo 2: Características, elementos y funcionamiento **4**
2.2. Elementos 6
2.3. Funcionamiento 9
2.4 Fundamento criptográfico 17
2.5 Garantías de seguridad 24
2.6. Recomendaciones de uso establecidas 27
Capítulo 3: Vulnerabilidades y amenazas de seguridad **29**
3.1. Asociadas al uso de recursos de operación 29
3.2 Herramientas 30
3.3 Inherentes al funcionamiento de Bitcoin 30
3.4 Fraudes y ataques 40
Capítulo 4: Situación legal y comercial **42**
4.1 Nivel regulatorio 42
4.2. Aceptación y uso comercial 43
Capítulo 5: Análisis **44**
5.1 Ventajas y Desventajas 44
5.2. Retos 45
5.3. Iniciativas 45
Conclusiones **47**
Glosario **48**
Anexos **51**
Bibliografía Específica **54**
Bibliografía General **57**

Índice de tablas y figuras

Lista de Tablas

Tabla 1. Ejemplo de criptodivisas 2
Tabla 2. Vulnerabilidades en el protocolo Bitcoin con mayor puntuación 39

Lista de Figuras

Figura 1. Infografía: Cómo funcionan las transacciones de Bitcoins 10
Figura 2. Detalle de la cadena de bloque 11
Figura 3. Componentes de un bloque 12
Figura 4. Estructura de las transacciones. 13
Figura 5. Árbol de Merkle y cadena de bloques 15
Figura 6. Funcionamiento POW 16
Figura 7. Verificación de origen, generación de direcciones y transacciones 18
Figura 8. Firma digital de transacciones 19
Figura 9. Generación de direcciones en Bitcoin 21
Figura 10. Funcionamiento de *Pay-To-Public-Key*-Hash (P2PKH) 22
Figura 11. Encadenamiento de elementos en el proceso 23
Figura 12. Ataque kleptográfico al ECDSA aplicado a Bitcoin 32
Figura 13. Funcionamiento del ataque de maleabilidad de transacciones 35
Figura 14. Diagrama de ataques de doble gastos 37
Figura 15. Información sobre vulnerabilidades reportadas en el protocolo.... 38

Agradecimientos

A mi familia y amistades por la paciencia y el apoyo brindado al realizar esta especialización.

A Francisco Dosca, Andrés Chomczyk y Horacio Hernández por la información proporcionada durante las charlas de ONG Bitcoin Argentina.

A Óscar Retana de Gridshield por los contactos y datos proporcionados sobre la situación actual de Bitcoin en Costa Rica.

A Hugo Scolnik, Néstor Masnatta, Pedro Hecht y Myrian Errecalde por sus aportes a la corrección y mejora del documento.

Nómina de abreviaturas

ATM: *automatic teller machine*, cajero automático.

ASIC: *application-specific integrated circuit* o circuito integrado para aplicaciones específicas.

BTC: unidad común de la criptodivisa Bitcoin.

CPU: *Central processing unit* o unidad central de procesamiento.

DDoS/DoS: *Distributed Denial of Service/ Denial of Service attack*, ataque de denegación de servicio.

DNS: *Domain Name System*, sistema de nombre de dominios.

DSA*: Digital Signature Algorithm*, algoritmo de firma digital.

ECDSA: *Elliptic Curve Digital Signature Algorithm* o algoritmo de firma digital con curvas elípticas

FPGA: *field-programmable gate array* o matriz de puertas programables.

GPU: *graphics processor unit*, unidades de procesamiento gráfico.

IP: *internet protocol address*, dirección del protocolo de internet.

P2P: Plataforma *peer-to-peer*, plataforma par-a-par.

POW*: proof-of-work*, prueba de trabajo.

RIPEMD-160: *Race Integrity Primitives Evaluation Message Digest* función *hash* con longitud de salida de 160 bits.

SHA256:

Tx: transacción.

TxID: identificador de la transacción o *Transaction Identifier.*

Introducción

Las criptodivisas han ganado terreno en los últimos años, por lo tanto, es oportuno investigar su impacto y riesgos asociados dada la importancia que tendrán, suponiendo que su uso se extienda[1]. Debido a la popularidad creciente del tema, es fácil conseguir información en bases de datos y medios especializados, sobre todo del ejemplo con mayor difusión como es el bitcoin, razón por la cual se escoge esta opción para elaborar la investigación.

El estudio a elaborar se considera relevante pues tiene como objetivo identificar los riesgos de seguridad alrededor del uso de Bitcoin una vez comprendido el mecanismo de funcionamiento del protocolo, las prevenciones expuestas por los creadores del mismo y los problemas de seguridad encontrados hasta el momento. Se pretende extender el tema al entorno del ciudadano común latinoamericano en dos sociedades específicas (la argentina y la costarricense) y realizar un análisis holístico de la situación actual de la criptomoneda.

Esta investigación se estructura en capítulos, donde los dos primeros dan un panorama de las criptodivisas y explicaciones del protocolo Bitcoin con especial énfasis en su fundamento criptográfico, a fin de comprender el objeto de estudio. Seguidamente, en los capítulos 3 y 4 se ahonda en el tema de vulnerabilidades, amenazas y situación en los países escogidos. Finalmente, en el capítulo 5 se analiza la información y se concluye sobre las implicaciones de seguridad en torno al uso de las Bitcoin.

[1] Según un reporte de *Goldman Sach* el uso de Bitcoin podría cambiar, junto con otras tendencias del mercado, la mecánica transaccional actual y con ello el futuro de las finanzas [1].

Capítulo 1: Estado del arte de las criptodivisas

1.1. Definición criptodivisa, tipos y ejemplos

Criptomoneda/criptodivisa es la divisa digital que utiliza una red *peer-to-peer* como medio de intercambio y usa fundamentos criptográficos para garantizar la seguridad en su uso. Se caracteriza por ser descentralizada, con costos de operación bajos y medios para garantizar la privacidad, entre otras particularidades que la distinguen de otros medios de pagos digitales.

La mayoría de las criptodivisas que han surgido siguen el modelo funcional propuesto por Satoshi Nakamoto[2] con Bitcoin, se basan en su código abierto, pero se distinguen por utilizar diferentes primitivas criptográficas o tener finalidades particulares [2]. A estas monedas virtuales derivadas se les conoce como *altcoin*, existen más de 63[3] pero solo se exponen cuatro ejemplos que se muestran en la Tabla 1.

Tabla 1. Ejemplos de criptodivisas

	Bitcoin	**Litecoin**	**Namecoin**	**Peercoin**
Función Hash	*SHA-256*	*Scrypt*[4]	*SHA-256*	*SHA-256*
Protocolo/ Esquema	*Proof-of-work*			*Proof-of-stake Proof-of-work*
Confirmación (min)	10	2,5	10	10
Valor U$S/moneda	291,31	2,03	0,5	0,40
Límite monedas	21 millones	84 millones	21 millones	ilimitada
Ventaja	La de mayor difusión y aceptación.	Rápidos tiempos de transacción.	Diversas funciones: DNS, internet sin censura, etc.	Menor gasto energético en minería.
Desventaja	Alto gasto energético en minería.	Dispositivos FPGA y ASIC necesarios son más caros y complicados.	Internet sin censura puede ser utilizado para actividades ilegales.	-Puntos de control centralizados. -Todo envío de monedas tiene un costo.
Particularidad	Primera criptodivisa	Proof-of-work se realiza en las GPU[5]	Trabaja como DNS	Diseñada para tener 1% de inflación

[2] En el 2008 publica el *paper* que da origen al modelo y en el 2009 se libera el primer software Bitcoin.
[3] Según coinmarketcap.com
[4] Función de derivación de claves basada en contraseña, diseñado específicamente para que sea costoso realizar un ataque al exigir grandes cantidades de memoria.
[5] GPUs tienden a tener mucho más poder de procesamiento en comparación con la CPU [4].

Para efectos de esta investigación, no se ahondará en todas las primitivas criptográficas ni procesos indicados en el cuadro anterior ni en las *altcoin* en general, solo se detallarán aquellos aspectos relacionados con Bitcoin.

1.2. Estado actual

A nivel comercial, si bien más establecimientos físicos y virtuales están aceptando estas divisas como medio de pago (se espera un incremento del 23% de aceptación en comercios en los próximos 2 años[6] y se triplicaron los proyectos basados exclusivamente en BTC alrededor del mundo[7]), la tendencia no se ha generalizado. En Europa, Asia y Estados Unidos, su uso es más frecuente pero en Latinoamérica su difusión y utilización ha sido menor. Sin embargo, estas divisas ya tienen una postura oficial positiva[8] por varios gobiernos[9] y la aceptación como medio de pago por grandes empresas como *Paypal*, *Dell, Microsoft,* entre otras [3].

Por otro lado, aunque es una iniciativa ya consolidada y en crecimiento, últimamente ha sufrido varias situaciones que afectan la confianza en su uso: *hackeo* de direcciones, robo de cuentas, fraudes, utilización para lavado de dinero, negocios ilícitos o pago de *ransomware*, la quiebra de intermediarios importantes, entre otros aspectos y hechos que se analizan a lo largo de este trabajo para validar las implicaciones de seguridad asociadas al uso de este método de pago.

[6] Según datos de Electronic Transactions Association [3]

[7] Según Pantera Capital, durante 2014 se realizaron más de 4500 proyectos basados exclusivamente en Bitcoin (tres veces más que el año anterior) y la inversión privada recibida por empresas del sector superó los 300 millones de dólares [3].

[8] No se considera como moneda legal (no se puede pagar impuestos con ella) pero no se ha expresado explícitamente la desaprobación o persecución por su uso.

[9] Exceptuando Noruega, Vietnam, Islandia, Rusia, Kirguistán, Bolivia y Ecuador [3].

Capítulo 2: Características, elementos y funcionamiento

La plataforma utilizada por Bitcoin se distingue por el uso de tecnología *peer-to-peer,* la cual permite la comunicación directa entre usuarios de manera colectiva sin necesidad de un ente central. Gracias a esto se logra la descentralización, escalabilidad y redundancia de la red.

Además de tener comunicaciones descentralizadas, Bitcoin se caracteriza porque no depende de ninguna entidad para la emisión, control y distribución de las criptodivisas, son los nodos que conforman la red Bitcoin quienes mediante una estructura robusta y simple se encargan de realizar estas tareas. Estos trabajan al mismo tiempo con poca coordinación, sin necesidad de identificarse, sin obligación de permanecer asociados a la red, se comunican entre sí al mejor esfuerzo pero con reglas de consenso que permiten mantener el orden y la seguridad en toda la estructura.

Con respecto a la seguridad, es importante recalcar que este aspecto se garantiza principalmente por el uso de protocolos criptográficos, es decir, la seguridad de las transacciones no se basa en la confianza mutua, sino en fundamentos criptográficos como firmas digitales entre otras primitivas.

Asimismo, al tratarse de una divisa, la criptomoneda bitcoin posee características especiales, como por ejemplo ser considerada una divisa volátil pues su valorización puede crecer/decrecer debido a que depende de la oferta/demanda y la especulación. En teoría, esta volatilidad se reducirá conforme el mercado y la tecnología Bitcoin maduren.

Un aspecto a favor de esta moneda es la dificultad de falsificación. Al estar compuesta por una cadena de firmas digitales, falsificar o adulterar las bitcoins resulta más difícil en comparación con otros medios de pago electrónico o el dinero en efectivo común. Además, al carecer de representación física real[10], su falsificación física es absurda. Por otro lado, la red Bitcoin funciona sobre la teoría de la oferta de divisas controlada, donde el suministro de BTC se controla mediante la creación de bloques. Dado que el número máximo de BTC que se puede generar es de 21 millones, la banca de reserva fraccionaria será como máximo 21 x 1014 unidades de moneda

[10] Existen representaciones físicas de BTC llamadas monedas *Casascius* pero en realidad son contenedores de las direcciones, no tienen valor en sí.

como oferta de dinero [5]. Con este modelo, se pretende evitar la pérdida de poder adquisitivo por inflación.

Además, dado que la divisa carece de curso legal forzoso (a diferencia de las monedas fiduciarias de cada país) el bitcoin es utilizado únicamente por quienes participan en el sistema. Esta participación es voluntaria y se aplica en cualquier parte del mundo.

Otra particularidad de esta moneda es la diversidad de la adquisición: pueden conseguirse monedas al minar, al aceptar bitcoins como pago por un servicio/producto dado o al comprarlas a un intermediario con moneda fiduciaria (dólar, euro, pesos, colones, yenes, yuan, etc.).

Finalmente, la tipificación financiera es una característica dual de la criptodivisa pues es considerado dinero (se pueden realizar transacciones económicas con él) y también título de valor (debido a las fluctuaciones de cotización respecto al dólar es adquirido para especulación) [6].

Por otro lado, la plataforma Bitcoin se distingue también por poseer transacciones con características particulares. Por ejemplo, toda transacción es irreversible, es decir, una vez que la transacción es realizada, no se puede revertir, solo pueden ser reembolsadas por la persona que recibe el pago. Una característica que catapultó la fama de Bitcoin fue su supuesto anonimato, pero cabe aclarar que en realidad las transacciones son privadas pero no anónimas: si bien es posible realizar transacciones sin revelar la identidad del emisor/receptor, las transacciones pueden ser rastreadas y analizadas de manera que se puede deducir el historial financiero de cada parte [7]. Este mecanismo de rastreo se logra gracias a la transparencia de las transacciones, pues las mismas están registradas y disponibles en línea para el monitoreo y escrutinio del público en general [7]. Otras características que atraen sobre las transacciones en la red Bitcoin es el bajo costo de las comisiones por operación y la posibilidad de realizar micro-transacciones. La primera característica se basa en el bajo costo por transacciones comparado al costo operacional con entes centralizados como bancos, tarjetas de crédito, etc. [2]. El costo puede ser nulo, aunque una comisión puede garantizar que la transacción sea confirmada con mayor velocidad. La segunda característica, las micro-transacciones, se utilizan principalmente para el pago de comisiones a mineros, propinas o donaciones. Son

transacciones de fracciones de BTC, fracciones llamadas *Satoshi* que equivalen a 10^{-8} BTC [7].

Es importante recordar que las transacciones son rápidas y a nivel internacional: en cuestión de minutos es posible disponer del dinero transaccionado desde cualquier punto del planeta, solo se requiere tener una conexión a internet.

Por último, el matiz legal de la plataforma, la divisa y las transacciones es un tema todavía en discusión debido a que no es una moneda oficial y su aceptación o regulación depende del país donde se utiliza. Actualmente, entre los no detractores de las criptodivisas existen dos tendencias de consideración regulatoria: por una parte, se les considera como moneda privada (como dinero pero no de curso legal forzoso) y la otra donde se le toma como un instrumento financiero y no como dinero *per se* [8].

2.2. Elementos

El término bitcoin se refiere tanto a la criptodivisa como al protocolo, la red peer-to-peer utilizada y al software de gestión[11]. A continuación se presenta una breve descripción de los elementos de Bitcoin.

- **Transacciones:** proceso por el cual se transfieren las criptodivisas, especifica cuántas BTC fueron tomadas de cada dirección emisora y cuántas fueron acreditadas a cada dirección receptora.

- **Transacción *Coinbase***: Un tipo especial de transacción sin *inputs*, creada por los mineros, es la primera transacción del bloque y solo existe una de su tipo en cada bloque. Su función es otorgar la recompensa al minero por el trabajo realizado (comisiones por transacción o el pago por bloque).

[11] Aclaración: bitcoin con b minúscula denota a la criptodivisa, Bitcoin con b mayúscula denota al protocolo, la red y el concepto.

- **Confirmación:** acción de procesar y verificar una transacción, realizada por los nodos de la red. Las transacciones son confirmadas cuando son incluidas en un bloque.

- **Bloque/*Block:*** registro permanente que contiene las confirmaciones de transacciones pendientes, un número aleatorio (*nonce)* y un hash del bloque anterior. En promedio, cada 10 minutos, un nuevo bloque que incluye nuevas transacciones se anexa a la cadena de bloques a través de la minería. El primer bloque creado se llama “Génesis” [2].

- **Banco de memoria/*Memory Pool (mempool):*** estructura local en cada nodo con todas las transacciones recibidas y aún no confirmadas. Si una transacción que aparece en el *memory pool* de un nodo específico es confirmado en otro lugar, la transacción se elimina de ese *memory pool* [9].

- **Cadena de bloques/*Block chain**:*** registro cronológico de todas las transacciones realizadas y confirmadas en la red Bitcoin. Esta base de datos es pública, compartida y creada de forma colectiva por todos los nodos de la red, es el medio por el cual se verifican las transacciones y se evita el doble gasto de las BTC [2].

- **Mineros:** son los nodos especializados encargados de confirmar las transacciones mediante la minería de bitcoins [2].

- **Minería de bitcoins:** es el proceso de generación de nuevas divisas[12] y de verificación de las transacciones en la red de Bitcoin. La verificación corresponde a un sistema de consenso distribuido mediante el cual los mineros otorgan procesamiento de CPU o GPU de sus equipos computacionales para resolver problemas matemáticos del esquema de *proof-of-work* utilizados para garantizar la seguridad y funcionalidad de la red.

[12] Al minar exitosamente un bloque, se acuñan nuevas monedas que se otorgan como recompensa (pago del bloque) al dueño del bloque minado [7].

- **Direcciones/*Address*:** concepto similar a una dirección física o correo electrónico, cada usuario puede poseer una cantidad ilimitada de direcciones, caracterizadas por ser el hash de una clave pública ECDSA. Estas se utilizan para las transferencias de BTC, pues es la única información que se debe brindar al receptor de transacción.

- **Monederos/billetera (*wallet)*:** archivo contenedor de la clave privada de una dirección en particular, la cual se utiliza para firmar la transacción y garantizar tanto el origen de esta como su integridad. Cada monedero puede mostrar la cantidad de bitcoins que contiene (balance de BTC) y permite pagar una cantidad específica a una o varias direcciones. Los monederos pueden ser en línea (gestionada por una empresa como un servicio a través de un navegador) o como un software cliente instalado en un dispositivo (*smartphone, desktop,* etc.).

- **Velocidad de hasheo (*hashrate*):** unidad de medida de la potencia de procesamiento de la red Bitcoin.

- ***Script***: sistema de *scripting* para las transacciones, que es esencialmente una lista de instrucciones grabadas en cada transacción donde el emisor puede crear requisitos muy complejos que el receptor debe cumplir con el fin de reclamar el valor del *input.* Ejemplo: *scriptPubKey o Public Key Script, scriptSig o Signature Script.*

- **Nodo completo (*Full node*):** es un programa que ayuda a la red de dos maneras: al realizar la validación completa de transacciones/bloques y al permitir a clientes ligeros transmitir transacciones a la red. Es un trabajo voluntario que mantiene robusta la red y que solo requiere que el usuario interesado instale el programa Bitcoin Core y lo mantenga corriendo con el puerto 8333 abierto.

- **Prueba de trabajo *(Proof-of-work/*POW):** básicamente es un proceso aleatorio que requiere en promedio de mucha prueba y error, es difícil

de ejecutar (en términos de costo/procesamiento/energía) pero genera una prueba válida de trabajo fácil de confirmar.

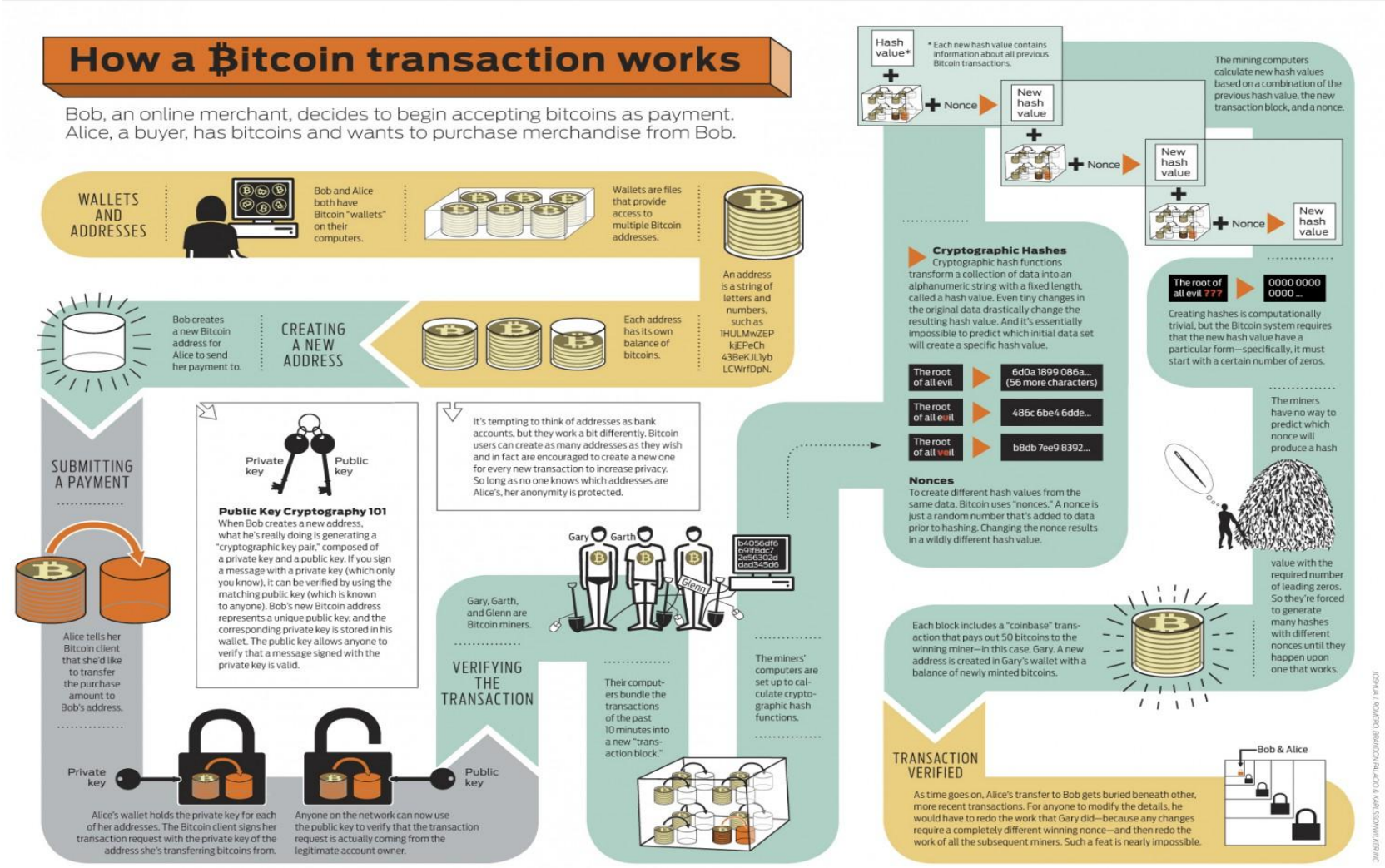
2.3. Funcionamiento

Como infraestructura necesaria para iniciar el proceso, ambas partes (el emisor y el receptor) deben contar con un monedero, conexión a Internet y el receptor debe enviar su dirección pública al emisor. El emisor inicia la transmisión de BTC desde su monedero, el cual genera una transacción, la firma con la llave privada (específica de esa dirección y de ese emisor) y lo difunde por toda la red para su validación[13] por parte de los mineros, quienes en caso de que la transacción sea válida, la registran localmente en el *memory pool* de cada nodo.

Al "minar" este bloque, los mineros en realidad están prestando la capacidad de procesamiento de su equipo computacional para encontrar un hash que cumpla con el nivel de dificultad de la prueba de trabajo (POW). Cada nodo se encarga de construir un bloque, al cual si se logra encontrar la respuesta al reto[14] del POW, se le incluyen todas las transacciones del *memory pool* y se transmite a la red. Si la red acepta el bloque, este es añadido a la cadena de bloques y los demás nodos utilizan el hash de este bloque como hash previo del siguiente bloque en la cadena.

En la Figura 1 se muestra una infografía que resume este proceso. Seguidamente se explica con más detalle la estructura de los componentes, los procesos de minería, la prueba de trabajo y el enlazamiento de las transacciones y la cadena de bloques.

[13] La validación corresponde a verificar que las transacciones sigan el formato correcto y que las BTC no se han gastado previamente.
[14] La respuesta del reto POW es el *nonce* (número aleatorio) con el que se logra llegar al hash del nivel de dificultad (detallado en el campo bits en el *block header*).

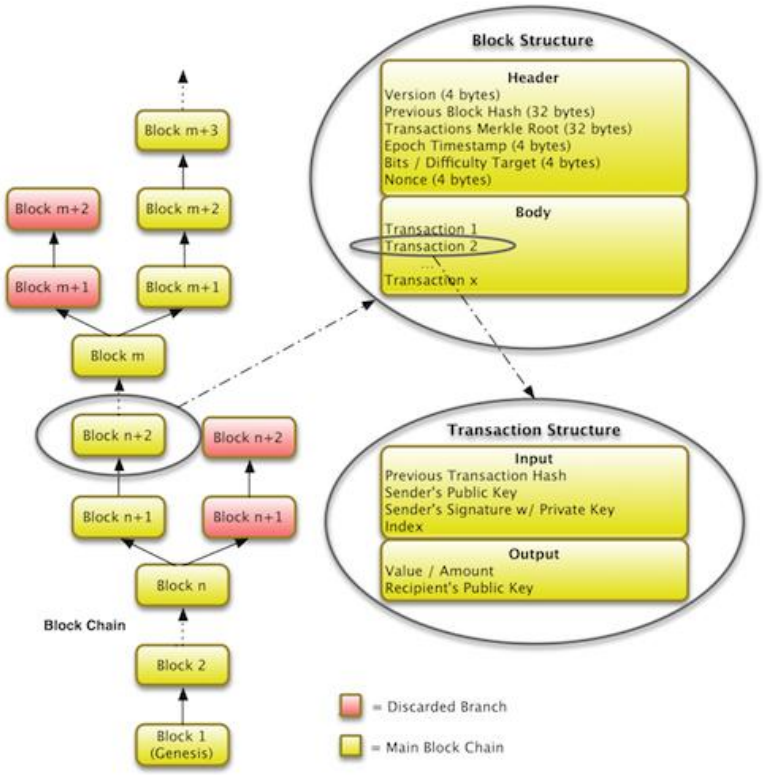


Fuente: http://visual.ly/bitcoin-infographic

Figura 1. Infografía: Cómo funcionan las transacciones de Bitcoins

Cadena de bloques: el orden cronológico y la garantía de integridad de los registros de las transacciones es fundamental en la red Bitcoin, aspectos que se logran con la aplicación de una función hash a las transacciones mientras se agregan a una cadena de pruebas de trabajo (POW) con el fin de colocarles una marca de tiempo (*timestamp*) y a su vez enlazarlos de manera que, para modificar algún elemento del registro, se deba de rehacer la prueba de trabajo. El registro resultante es la cadena de bloques *(block chain*). El proceso para generar esta cadena de bloques constituye una plataforma de coordinación segura, escalable, abierta y global que es la base del sistema descentralizado y distribuido de Bitcoin.

Una copia completa de la cadena de bloques contiene todas las transacciones realizadas desde la creación del protocolo, pero para el funcionamiento diario de la red, los nodos pueden trabajar con la copia del hash de la cabecera del bloque de la cadena más larga, la cual por reglas de consenso de la red, debe ser la utilizada para añadirle los bloques con las nuevas transacciones aceptadas. En la Figura 2 se muestra la cadena de bloques, la estructura de los bloques y las transacciones.

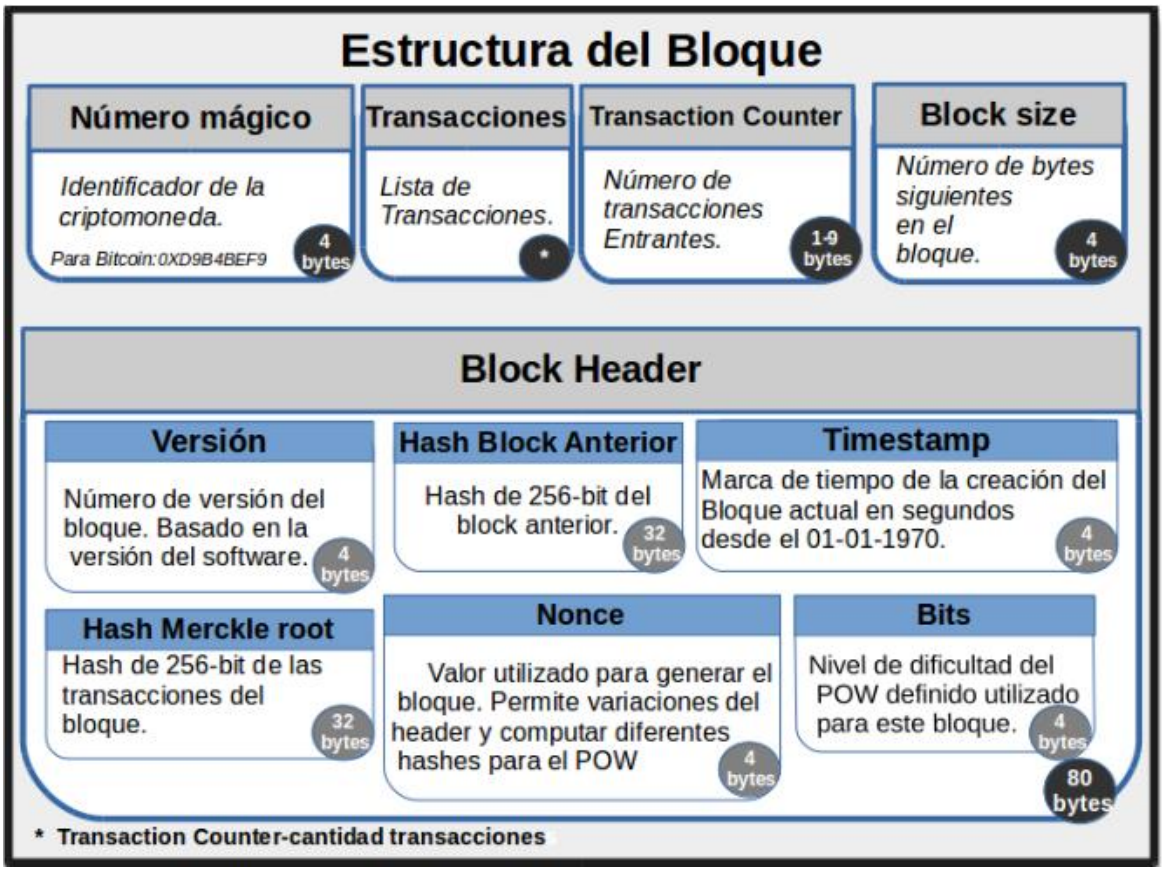


Fuente: [5]

Figura 2. Detalle de la cadena de bloque

En la figura anterior se muestra una bifurcación de la cadena, la cual se le conoce como *Fork*. Esta bifurcación suele suceder durante el cambio de las reglas de consenso, cuando hay un periodo donde los nodos están desorientados.

Bloques*/ blocks*: son los contenedores de las transacciones (pueden incluir alrededor de 500). Mediante el *hash* del bloque anterior (referencia) se entrelazan formando la cadena de bloques. En la Figura 3 se presentan las partes del bloque y a la vez, se describe la cabecera del bloque o *Block Header*.

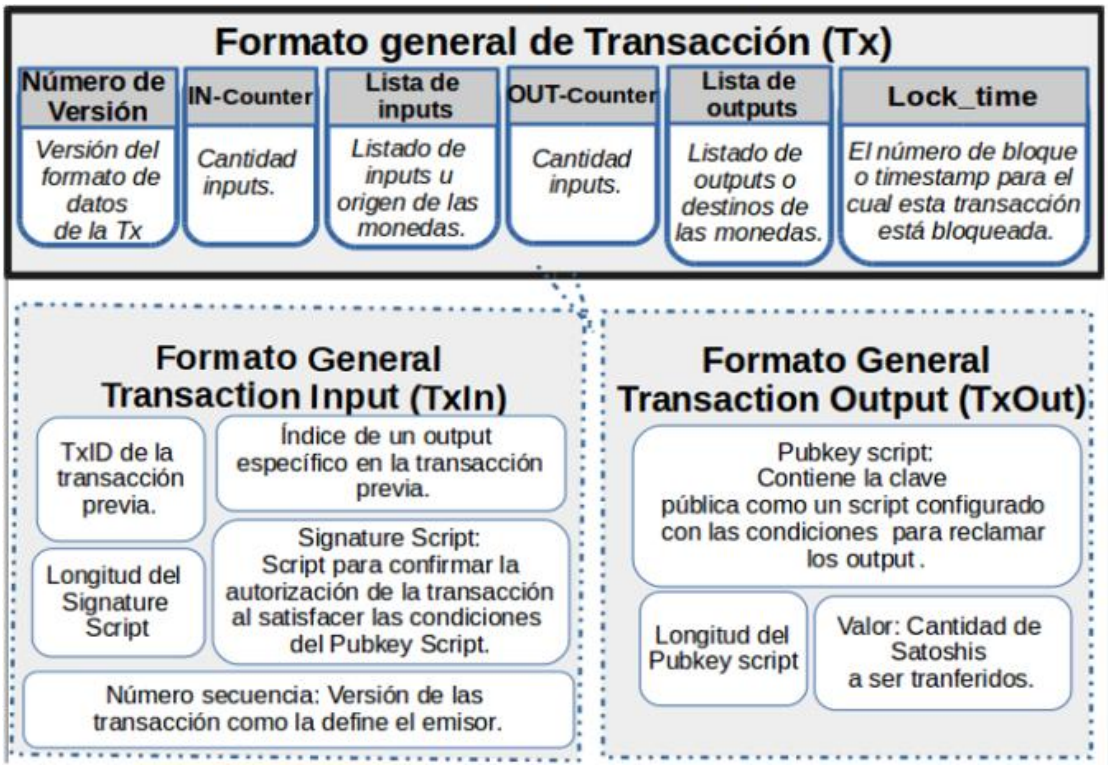


Fuente: Elaboración propia basado en información de [2].

Figura 3. Componentes de un bloque

Transacciones: las transacciones están compuestas por *output* e *inputs* para la combinación y separación de los valores. El *input* es el dato con el origen de la moneda (referencia con el *output* de la transacción anterior) mientras

que el *output* está ligado con la referencia de la transacción (el identificador o TxID, es decir, el *hash* de la transacción) e indica la cantidad disponible de monedas y la dirección del receptor de la transacción. Los *outputs* se clasifican en dos tipos: transacción de salida no gastada (*unspent transaction output*/UTxO) y gastada (*spent transaction output*/StxU) [2]. En la Figura 4 se muestran las partes de las transacciones.



Fuente: Elaboración propia basado en información de [2]

Figura 4. Estructura de las transacciones.

Cabe resaltar las funciones específicas de algunas partes: el número de versión de la transacción le indica a los nodos cual set de reglas de consenso utilizar para la validación, el *lock_time*[15] y el número de secuencia demuestran si la transacción está finalizada[16], los *inputs* utilizan el TxID y el índice del *output* para identificar el *output* específico que debe ser gastado y el *Signature Script* proporciona los parámetros de datos que satisfacen las condiciones del *Pubkey Script* [2].

[15] Indica el primer momento en que una transacción puede ser añadida a la cadena de bloque y permite crear transacciones bloqueadas que solo serán válidas en el futuro, dando a los firmantes la posibilidad de cambiar de opinión (se inválida esa transacción si se crea una nueva transacción no bloqueada).

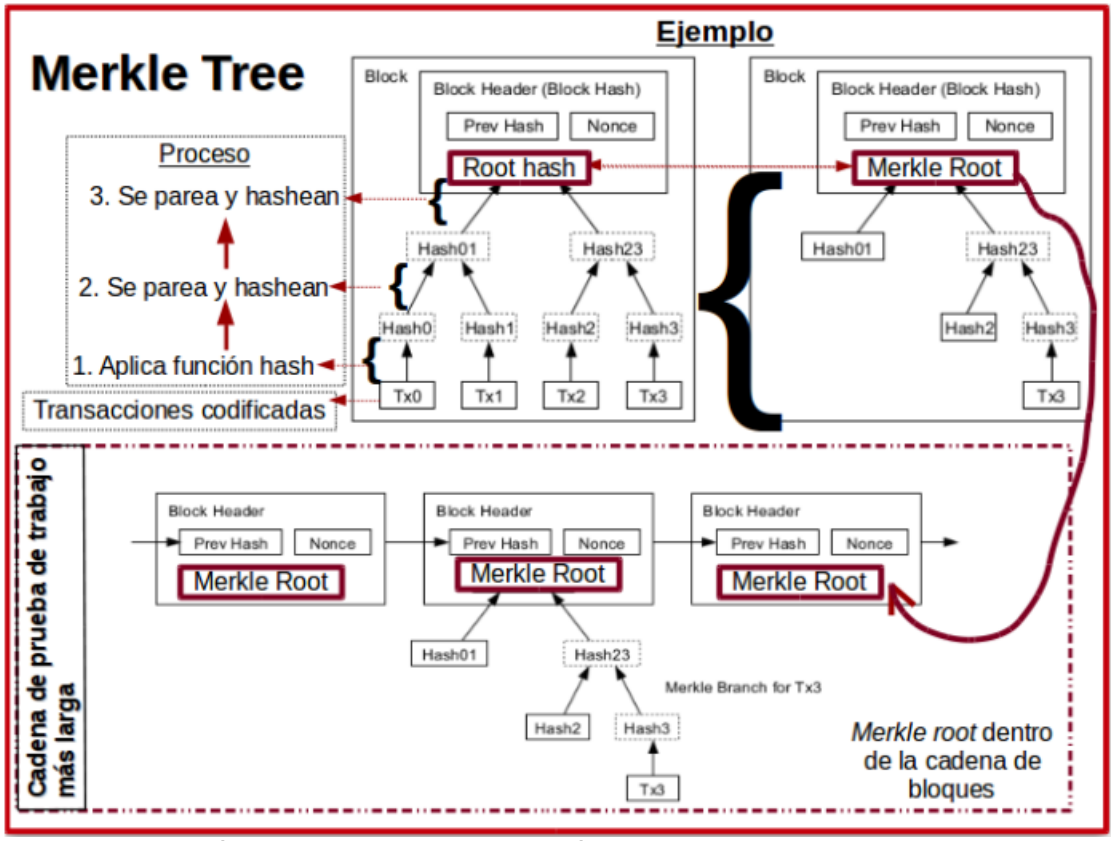
[16] Una condición de una transacción estándar es que esté finalizada, es decir, que el locktime sea menor/igual al *block height* actual o que todos los números de secuencia sean 0xffffffff.

Una transacción se considera inválida y por ende rechazada si [10]:

- Algún dato de la transacción es incorrecto o inválido.
- El output está categorizado como ya gastado o el input ya fue utilizado.
- La transacción es idéntica a otra (mismo número de identificación).
- Firma digital inválida.
- Formato inválido.

Cadena de transacciones: los *satoshis* se mueven de una transacción a otra. Cada transacción gasta las monedas recibidas en una o varias transacciones anteriores, de manera que se crea una cadena de transacciones donde el *input* de una transacción es el *output* de la transacción anterior. Si el valor del *output* es menor al *input* de la transacción, la diferencia es añadida al valor de la comisión del bloque para los mineros.

Además, todas las transacciones son codificadas en los bloques en un formato binario al cual se le aplica una función hash para crear el identificador de la transacción (TxID). Con estos datos, se crea un árbol de Merkle al aparear cada TxID con otro TxID, luego aplicarle una función hash. A continuación, en forma repetida, los hashes resultantes se vuelven a aparear y a aplicar una función hash hasta lograr un solo hash resultante, el llamado *Merkle Root.* El *Merkle Root* está incluido en el *Block Header* de cada bloque y se utiliza como compactador de transacciones, pues de los bloques viejos se guarda solo este hash como referencia de las Tx que lo originaron. Este mecanismo permite verificar que una transacción fue incluida en un bloque en particular y enlista los hashes intermedios desde un nodo completo sin quebrar el enlace de los hashes de los bloques. En la Figura 5 se representa el árbol Merkle y su inclusión en *block header* [2].



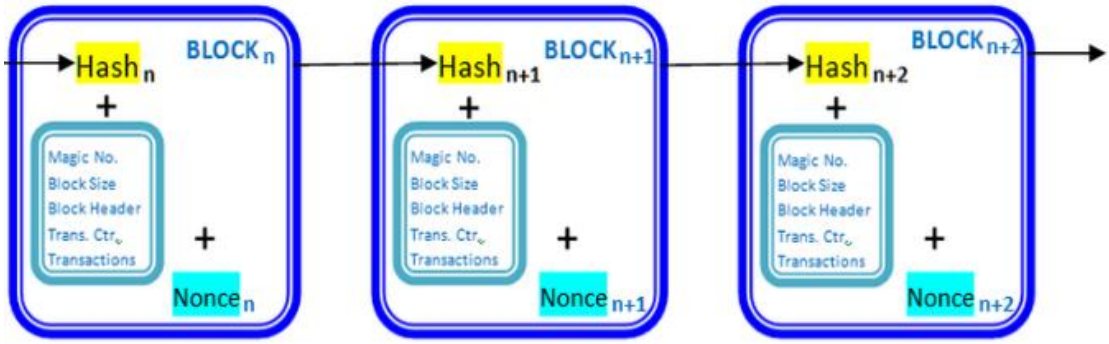
Fuente: Elaboración propia basado en información de [2]

Figura 5. Árbol de Merkle y cadena de bloques

Minería y Prueba de trabajo (POW): la prueba de trabajo garantiza dos aspectos necesarios para el funcionamiento de la red: primero, la determinación de la mayoría en la toma de decisiones (un procesamiento otorgado para el POW es equivalente a un voto en la evolución de la cadena de bloques y la validación de transacciones) y segundo, implementa el servidor distribuido de marcas de tiempo en la red P2P (necesario para mantener el registro cronológico y evitar el doble gasto de las monedas) [2].

Este esquema funciona como un reto-respuesta: el reto es generar un hash con una cantidad de ceros determinada con la información del hash del *block header* (hash que contiene todos las transacciones anteriores de la red), la información del nuevo bloque de transacción y el *nonce* que permite la generación de una nueva prueba (un nuevo *hash)*. Pueden existir múltiples respuestas (soluciones válidas para el bloque dado) pero solo se requiere

una, por lo que el primero que la obtiene y la transmite es quién gana la recompensa[17]. En la Figura 6 se representa el funcionamiento del POW.



Fuente: [11]

Figura 6. Funcionamiento POW

Una vez logrado el valor necesario que aplique al nivel de dificultad requerido, este hash se agrega al bloque, se transmite a los demás nodos quienes verifican que se cumple el reto y se agrega a la cadena de bloque en caso de ser aceptado por la red. Este proceso de resolver este reto es "minar", el cual al lograr un bloque exitoso, genera nuevas monedas que son pagadas a los mineros como recompensa al trabajo.

Este proceso asegura que todos los participantes tengan una visión consistente de los datos de Bitcoin, pues cada 10 minutos se oficializa el ingreso de un bloque con el consentimiento de la mayoría de los nodos, quienes garantizan el rechazo de transacciones inválidas o conflictivas.

Verificación de pago simplificado: en este modo**,** los clientes Bitcoin se conectan a un nodo completo arbitrario, descargan solo los *blocks headers* de la cadena de POW más larga, verifican que los *blocks headers* se conecten entre sí correctamente y que la dificultad sea bastante alta. Luego, solicita las transacciones con patrones coincidentes particulares del nodo remoto (es decir, los pagos a sus direcciones) que proporcionan copias de esas

[17] La recompensa por minar son monedas nuevas. Actualmente el monto es de 25 BTC, pero en un inicio era de 50 BTC. Cada 210 000 bloques el monto de recompensa se disminuye 50%.

transacciones junto con una rama Merkle que los vincula con el bloque en el que aparecían. De esta manera, la estructura de árbol Merkle comprueba la inclusión sin necesidad de mostrar el contenido de todo el bloque [2] [12].

2.4 Fundamento criptográfico

Verificación de origen, generación de direcciones y transacciones

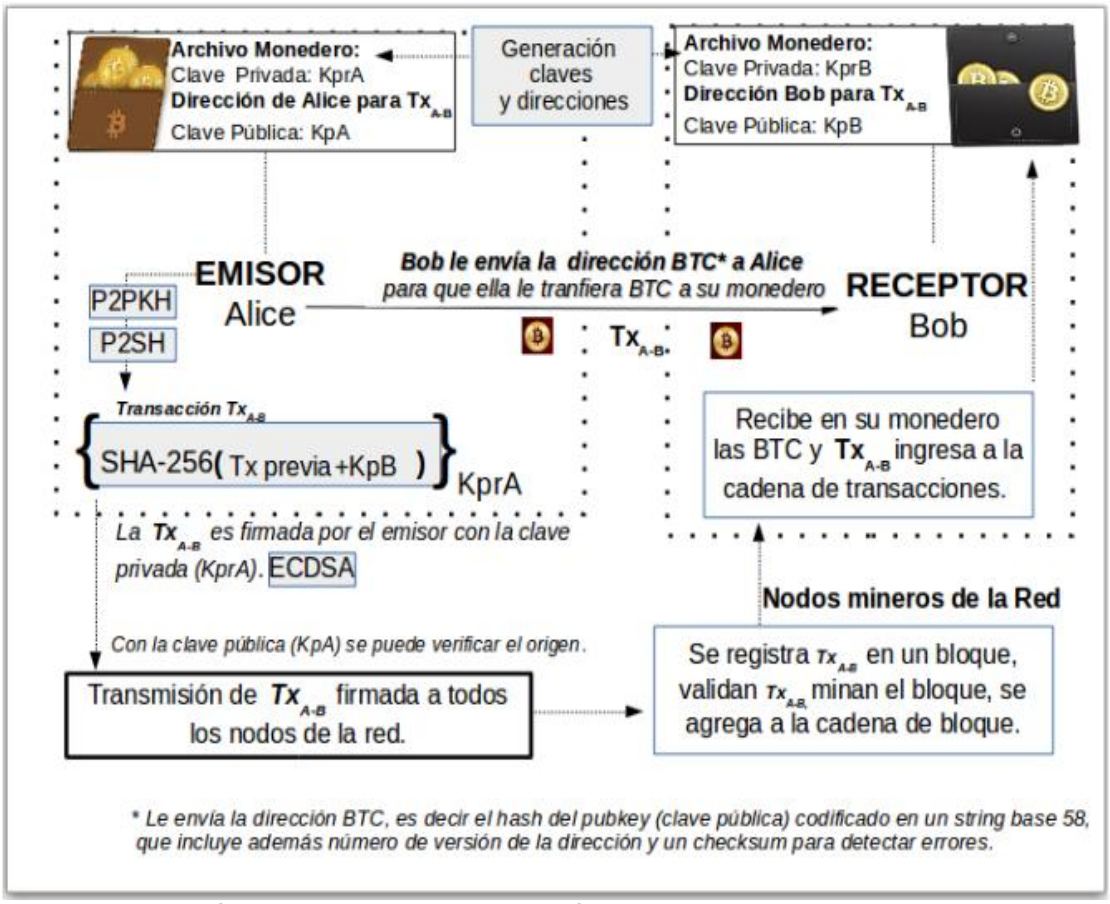
Se define la moneda electrónica en sí como una cadena de firmas digitales [2]. La firma digital permite la verificación del origen sin exponer la identidad del emisor o el receptor de la transacción. La transacción se firma con la clave privada asociada con la dirección del emisor y luego cualquier nodo de la red puede verificar con la clave pública que ese requerimiento de transacción proviene del dueño de esa dirección.

Se utiliza la criptografía de curvas elípticas tanto para la generación de direcciones como para la autenticación por firma digital. Específicamente se utiliza el ECDSA (*Elliptic Curve Digital Signature Algorithm*), el cual es una modificación del algoritmo de firma digital (*Digital Signature Algorithm*, DSA) donde se aplican operaciones sobre puntos de las curvas elípticas, concretamente “una instancia del problema de logaritmo discreto, la cual resulta mucho más compleja que el equivalente utilizado por los campos numéricos” [14]. De esta manera, se proporciona un sistema robusto, seguro y eficiente, ideal para dispositivos que disponen de pocos recursos computacionales. Actualmente, ECDSA es la opción recomendada pues en comparación con el sistema criptográfico RSA[18], posee mejores características para dispositivos de bajo consumo energético y mayor grado de dificultad frente a ataques[19].

En la figura 7 se explica el proceso de verificación del origen, generación de direcciones y transacciones con más detalle.

[18] Según datos proporcionados por Payeras et al, las firmas digitales utilizadas por el protocolo Bitcoin poseen una fortaleza equivalente a 128 bits con un tamaño de clave de 256 bits. En comparación, RSA/DSA requiere un tamaño de la clave de 3.072 bits para alcanzar el mismo nivel de seguridad [13].

[19] Hasta el momento se desconocen algoritmos de ataque que sean de complejidad subexponencial para la criptografía de curvas elípticas [14].



Fuente: Elaboración propia basado en información de [11] [2]

Figura 7. Verificación de origen, generación de direcciones y transacciones

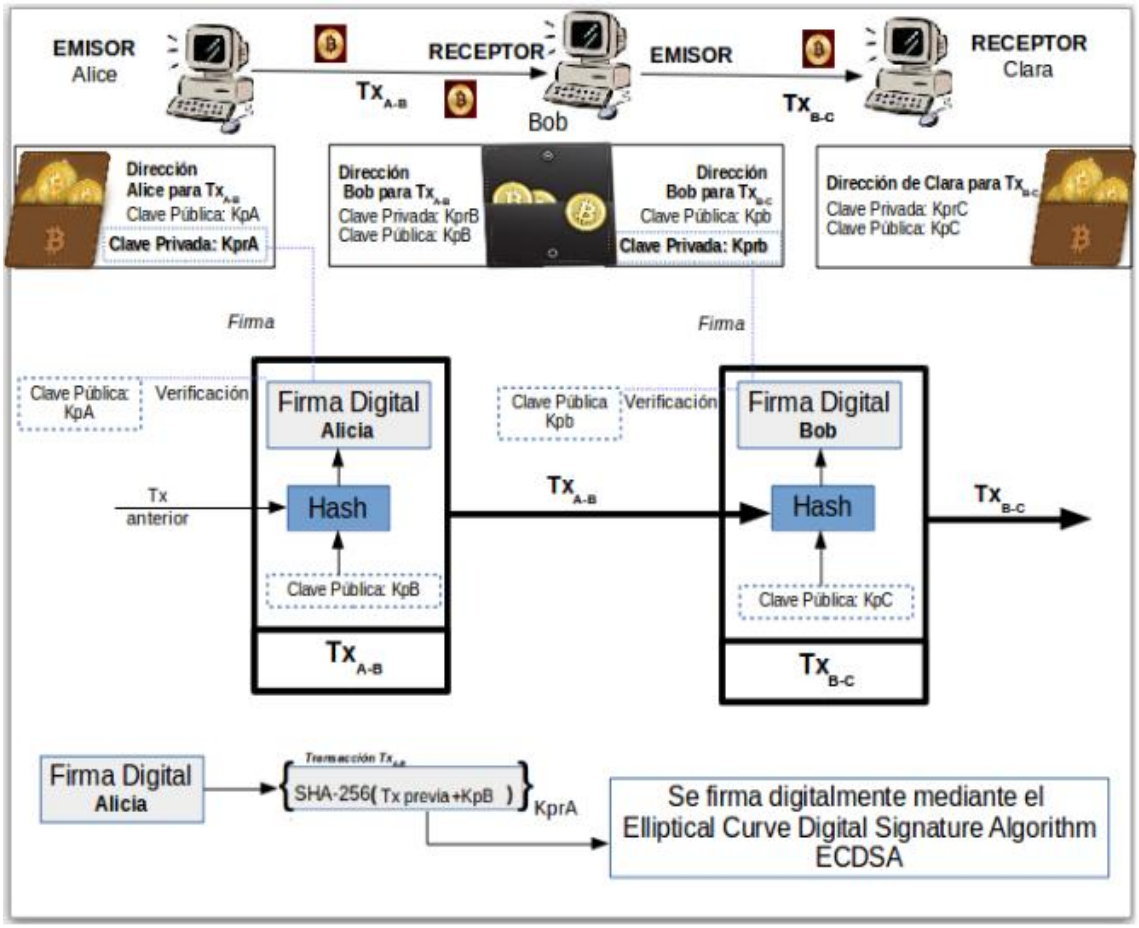
Para el protocolo Bitcoin, ECDSA utiliza la curva secp256k1 con la forma $y^2 = x^3+0x+7$, definida sobre el campo finito F_p donde $p= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, donde con el punto generador P de orden *n* es posible derivar la clave privada, la cual es un número aleatorio s<n y la clave pública es un punto de la curva que cumple Q=s•P.

La curva secp256k1 está definida por la *Standards for Efficient Cryptography* (SEC), es del tipo Koblitz[20] la cual tiene varias propiedades que la hacen útil para las funciones del protocolo, como poseer una forma especial no aleatoria que permite mayor eficiencia computacional (utiliza el método GVL -Gallant, Lambert and Vanstone [21]) y ser considerada una curva

[20] La curva Koblitz es una curva elíptica ordinaria $E : y^2 + xy = x^3 + a^2x^2 + 1$ sobre F_2

[21] El método GLV permite realizar cálculos mucho más rápidos cuando estas constantes son escogidas de acuerdo a ciertos criterios. Aunque existe la posibilidad de introducir debilidades al sistema por no escoger los valores al azar, actualmente no existen pruebas concretas de que las curvas no aleatorias en realidad sean más inseguras [15].

no manipulable debido a que las constantes seleccionadas para secp256k1 fueron escogidas de una manera predecible, lo que reduce la posibilidad de que el creador de la curva inserte algún tipo de puertas traseras o *backdoors*. En la Figura 8 se detalla el proceso de la firma digital con el uso de este algoritmo.



Fuente: Elaboración propia basado en información de [11] [2]

Figura 8. Firma digital de transacciones

Como se indicó anteriormente, la clave privada es generada aleatoriamente en un rango de valores válidos determinados por la curva secp256k1 y a partir de este valor se calcula la clave pública[22]. Como bien los indica Hecht [14]:

> "todas las aplicaciones criptográficas de la curvas elípticas están basadas en el producto escalar sobre un único punto P solución de la

[22] Es computacionalmente inviable conseguir la clave privada a partir de la clave pública si existe una correcta implementación/programación del protocolo y las partes asociadas.

> curva elíptica E y cuyo orden en el campo sea un primo(n) grande. En criptografía de clave pública, si 's' fuese una clave privada entonces su producto escalar s•P sería una clave pública"

Entonces, del rango de valores de la curva secp256k1 se escoge un valor aleatoriamente que representa a 's' y con él se calcula el producto escalar con el punto P, resultado que representa a la clave pública Q.

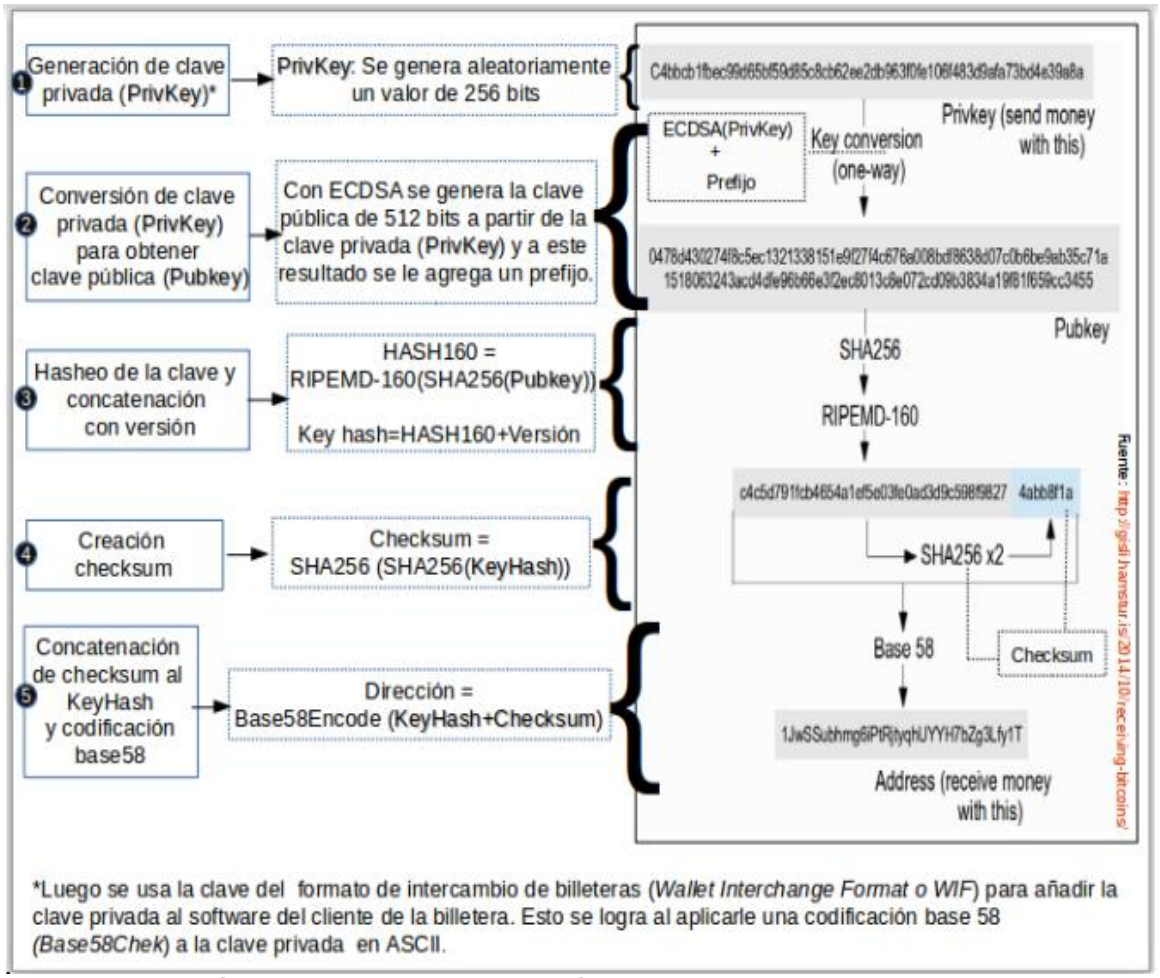
Para el caso concreto del protocolo Bitcoin, se le agrega a la clave privada un prefijo para generar símbolos distinguibles después de la codificación[23] y a la clave pública un *checksum* para evitar errores de manipulación de la dirección[24][16].

Finalmente, se realiza una conversión de la base 256 a la base 58, el cual es el formato de las direcciones bitcoin. En el código fuente del cliente Bitcoin, el creador del protocolo indica claramente la razón por la cual escoge Base58 en lugar de Base64: bajo este esquema de codificación, las direcciones pueden contener todos los caracteres alfanuméricos, excepto 0, O, I, y l para evitar problemas de ambigüedad [13].

En la Figura 9, se explica con detalle el proceso de generación de las direcciones.

[23] Existe una lista de estos prefijos-símbolos, pero los casos más conocidos son el prefijo 0 que genera el símbolo 1 al inicio de la dirección que significa un transacción tradicional y el caso del prefijo 5 que genera un símbolo 3 que significa una transacción compleja.

[24] Por ejemplo, al confundir una letra con otra al copiar una dirección impresa o si al copiar y pegar una dirección a través del portapapeles se hubiera copiado una dirección incompleta.

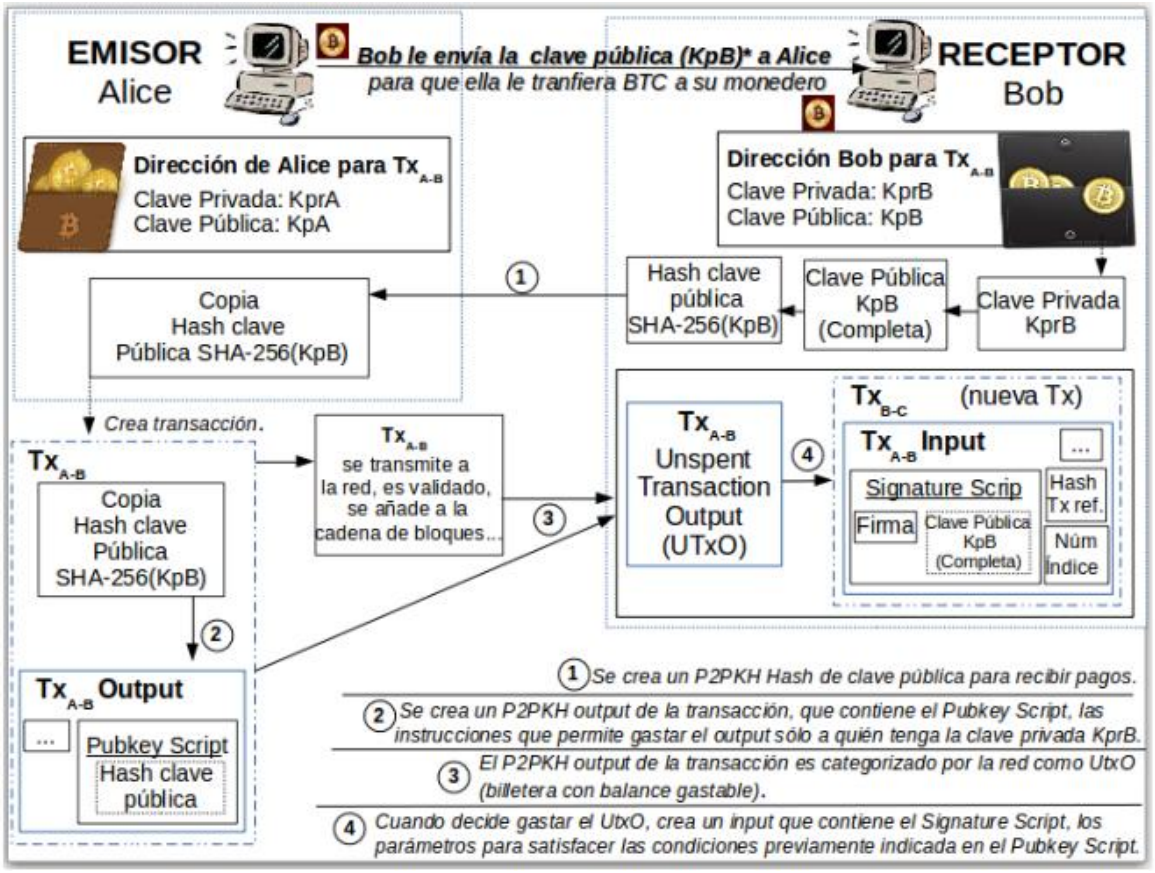


Fuente: Elaboración propia basado en información de [11] [13] [2], imagen de [12]

Figura 9. Generación de direcciones en Bitcoin

Por otro lado, la generación de transacciones tradicionales[25] se realiza por medio del estándar *Pay-To-Public-Key-Hash* (P2PKH), el cual combina condicionales lógicos, las instrucciones contenidas en el *Script* (compuesto por el *Pubkey Scripts y Signature Script)* y el algoritmo de curvas elípticas para crear un mecanismo de autorización programable. Este mecanismo de autorización permite que el *output* de la transacción solo sea gastado por quién posea la llave privada del receptor (se comprueba con el *Pubkey Script)*. En la figura 10 se muestra el funcionamiento de este estándar.

[25] Existen dos tipos de transacciones más: *Pay to Script Hash* (para transacciones no tradicionales, multi-fima) y *Generation*/Transacciones *Coinbase* (para generar monedas nuevas). Se explica solo el P2PKH porque es el más utilizado.



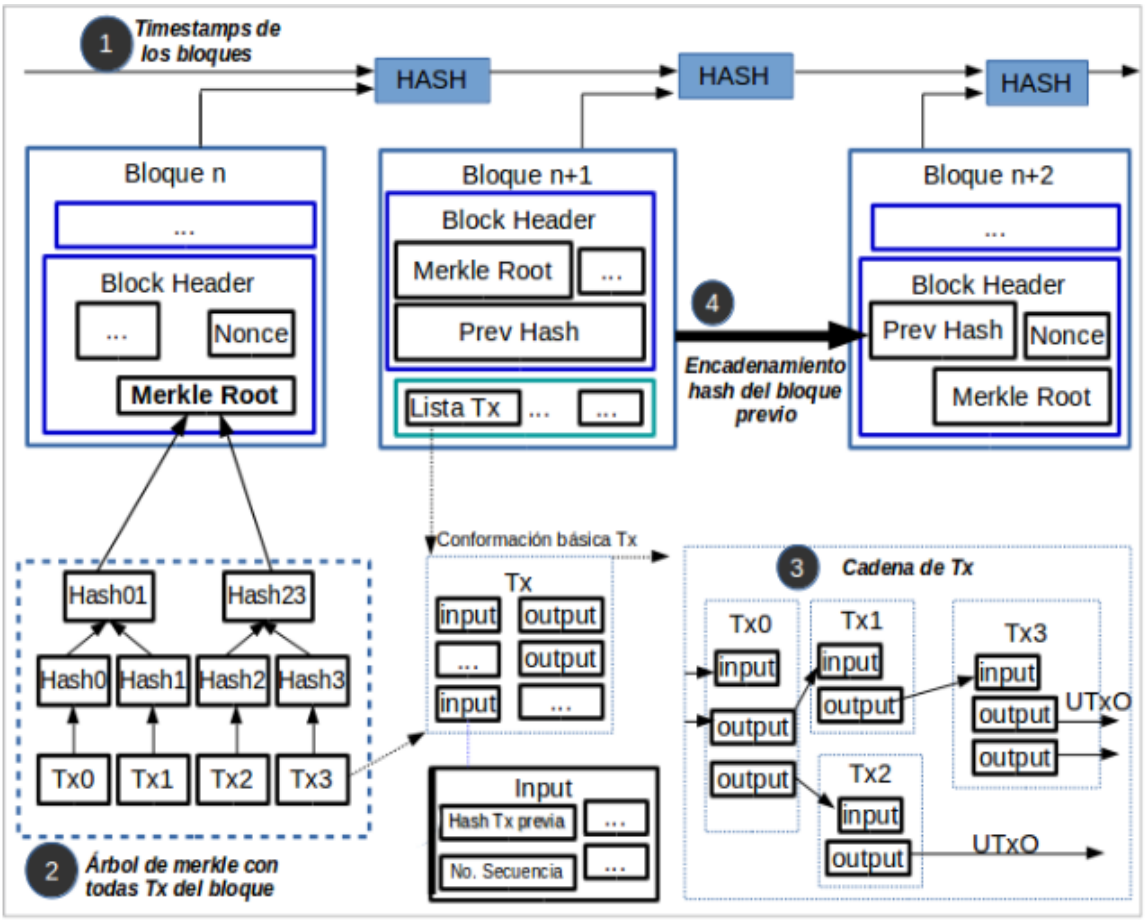
Fuente: Elaboración propia basado en información de Bitcoin Wiki.

Figura 10. Funcionamiento de *Pay-To-Public-Key*-Hash (P2PKH)

Encadenamiento de datos

Mediante el uso de funciones Hash (como SHA256 y RIPEMD-160) se logra comprimir los datos para añadirlos en componentes del protocolo para asociarlos con otros componentes, con el fin de enlazarlos en una gran cadena. Además, como bien se indica en la figura 9, se aplica dos veces el algoritmo de hash (o combinación de algoritmos) sobre los datos con el fin de generar un hash resultado que sea robusto y seguro contra el criptoanálisis.

En la figura 11 se muestran los diferentes enlaces entre datos mediante el uso de hashes y posteriormente se detalla cada entrelazamiento para su mejor comprensión.



Fuente: Elaboración propia basado en información de [11] [2]

Figura 11. Encadenamiento de elementos en el proceso

1. El servidor P2P distribuido de marca de tiempo (*timestamp*) se implementa utilizando POW incrementando un *nonce* en el bloque hasta lograr llegar a un hash con el nivel de dificultad del reto (un hash con una cantidad determinada de ceros). El hash del bloque anterior se guarda en el *block header* de cada bloque.

2. El uso de funciones hash para enlazar bloques y transacciones anteriores con un bloque/transacción en particular y el ahorro de espacio en disco cuando se utiliza el árbol de Merkle con el hash de las transacciones apareadas.

3. Todo *input* corresponde a un *output* y el entrelazamiento entre transacciones se realiza a través de un campo en los inputs. Cada

output de una transacción solo puede ser referenciado una vez por un *input* de una transacción subsiguiente.

4. Cada bloque en la cadena contiene un hash del bloque anterior creando así una cadena de bloques desde el primer bloque hasta el último bloque en la cadena más larga. Así se asegura que no puede ser modificado un bloque específico sin antes modificar el bloque que lo tiene registrado y todos los bloques subsiguientes a este.

2.5 Garantías de seguridad

Uno de los conceptos más importantes que establece el protocolo son las llamadas comisiones o incentivos[26] que se otorgan a los mineros con el fin de asegurarse su honestidad, pues les resulta mejor, desde el punto de vista financiero, apoyar a la red que atacar al protocolo [2]. Es decir, en caso de que un atacante logre mayoría en la cantidad de nodos en la red, será más beneficioso ganar las comisiones que se le darán por su trabajo que la ganancia por modificar bloques, confirmar transacciones inválidas o quebrantar el sistema. El costo computacional (gasto energético) que conlleva modificar un bloque en particular sobrepasa las ganancias que esta acción genera, pues el atacante debe alterar y rehacer el POW de ese bloque y los demás subsiguientes a este, además de lograr alcanzar a la cadena de bloques legítima y sobrepasarla para atacar con éxito a la red[27] [2].

Otro pilar del protocolo con respecto al tema de seguridad es el trabajo distribuido, colaborativo y regido por las reglas de consenso de la red. Mediante la participación sincronizada pero no premeditada[28] de los nodos en la red al aceptar o no procesar una transacción según lo establecido por las reglas de consenso, se mantiene la red estable pues se garantiza que los

[26] El valor del incentivo lo puede definir el emisor de la transacción o, en caso de que no sea una transacción *coinbase* y si el valor del input es menor al valor del output de esa transacción, la diferencia puede ser reclamada como comisión por el minero dueño ese bloque.

[27] En el anexo 1 se adjuntan los cálculos probabilísticos que Nakamoto incluye en el paper para justificar este punto.

[28] Es decir, cada nodo actúa según las reglas de consenso pero independientemente entre sí.

nodos trabajan siempre sobre las mismas premisas. Es importante resaltar que estas premisas son regularmente actualizadas y se tienen contramedidas para minimizar problemas por nodos desactualizados.

Por otro lado, se debe recordar que Bitcoin se basa en una red compuesta en su mayoría por nodos honestos. Según los fundamentos expuestos por Nakamoto en el *paper* original sobre Bitcoins [2], en el caso hipotético de que la mayoría de nodos en la red sean maliciosos y generen una cadena de bloques alternativa a la válida, el protocolo posee dos resguardos. El primero de ellos, el atacante solo puede revertir transacciones realizadas por él, no puede realizar cambios arbitrarios a otras transacciones ni direcciones pues existe una alta posibilidad de que algún nodo detecte el comportamiento nocivo del atacante y no acepte la transacción ni el bloque que contenga la Tx inválida[29]. El segundo de los resguardos es que mediante cálculos estadísticos se caracteriza la carrera entre una cadena deshonesta y una válida (por medio del método conocido como 'Camino aleatorio binomial' y el problema de la ruina del apostador o *Gambler's ruin problem) y* se determina que si el intento de doble gasto no se inicia inmediatamente después de que se haga la transacción original, la posibilidad de tener éxito se hace exponencialmente pequeña. En el anexo 1 se detalla el cálculo probabilístico realizado por Nakamoto que justifica la afirmación anterior.

A nivel técnico, la seguridad en comunicaciones y la red *peer-to-peer/*P2P son dos aspectos donde la criptodivisa se refuerza: en el primer caso los protocolos de pago usados por la red soportan los certificados X.509 y encriptación TLS para verificar la identidad de los receptores, encriptar comunicaciones entre nodos y así prevenir ataques *man in the middle*, etc., mientras que el segundo caso las redes P2P garantizan comunicaciones sin intermediarios, de manera directa entre nodos y permite que toda la información sea transmitida a todos los nodos. La redundancia que brinda el sistema P2P es fundamental, pues al ser tolerante a pérdida de mensajes no es necesario que alcance a todos los nodos para funcionar adecuadamente, pues se actualizan con el último *block chain* al aceptar como legítimo *el block chain* más largo en dificultad POW.

[29] Se puede implementar sistemas de alertas o contar con nodos propios para agilizar las transacciones y tener mayor seguridad [2].

A nivel de protocolo, se debe resaltar la actualización del nivel de dificultad del POW. La actualización consiste en que cada 2016 bloques se reevalúa el valor de dificultad del hash contra el cual se validan las confirmaciones. La red utiliza un marcador de tiempo guardado en cada *block header* para calcular el número de segundos entre la generación del primer y segundo de los 2016 bloques[30]. Si toma más de 2 semanas, la dificultad se incrementa proporcionalmente (hasta 300%) y si toma menos de 2 semanas el valor se reduce proporcionalmente (hasta un 75%), ambas medidas con el fin de lograr que la generación de bloques se realice exactamente con el misma tasa.

Finalmente, mediante la cadena de bloques/*Block Chain* es posible garantizar que no haya un doble gasto de una misma moneda ni modificación de los registros previos. En el caso del doble gasto, este se previene gracias al encadenamiento entre transacciones, pues el protocolo debe garantizar que esto suceda al permitir solo el uso de *outputs* clasificados como *unspent transaction* o*utput.* Por otro lado, la integridad de los bloques se garantiza gracias a la firma digital y al encadenamiento entre bloques, donde los hashes intermedios no pueden ser falsificados, pues en ese caso, la verificación de la transacción fallaría y esta sería rechazada. Con respecto a este tema, se considera que un ataque tiene poco rentabilidad económica pues al estar encadenados los bloques, la modificación de un bloque específico implica un alto costo para el atacante pues debe modificar todos los bloques que se han añadido al *block chain* después del bloque que desea modificar. Por lo tanto, el trabajo que requiere el atacante es mucho mayor al que requieren los nodos honestos para añadir nuevos bloques a la cadena, lo que puede resultar poco práctico para el atacante.

Por último, es importante recalcar que los softwares regulares de billetera Bitcoin encriptan las claves privadas con el AES 256-CBC y solo los descifran cuando el usuario desea crear una transacción.

[30] 2016 bloques son idealmente 1209600 segundos, es decir 2 semanas (14 días). Este parámetro fue definido por el creador del protocolo y corresponde a un aproximado de 1 bloque cada 10 minutos, lo que implica 6 bloques por hora, 144 bloques por día. Esa cantidad por 14 días es igual a 2016.

2.6. Recomendaciones de uso establecidas

Aspectos técnicos

Para mejorar el nivel de privacidad y anonimato en las transacciones, se recomienda usar TOR, una plataforma que permite enmascarar la dirección IP del usuario y TAIL, una distribución de Linux del tipo sistema operativo *live*, que obliga a realizar todas las conexiones utilizando TOR y permite cifrar correos, comunicaciones, etc.

Para evitar pérdidas importantes de monedas, se recomienda distribuir la cantidad de BTC en distintos medios**,** no guardar la totalidad en un solo monedero, manejar montos pequeños para el uso diario y mantener los ahorros en monederos *offline o cold storage*[31] con el respaldo, seguridad y encriptación adecuado. También, se recomienda utilizar la firma *offline* de transacciones que consiste en dos equipos que comparten partes del mismo monedero pero uno conectado a la red y el otro desconectado. El equipo conectado a la red solo puede crear transacciones sin firmar y equipo desconectado firma esa transacciones. Con esta medida, en caso de que el equipo con mayor posibilidades de ser vulnerado (el dispositivo *online*) sea comprometido, no es posible retirar fondos del monedero. Otra medida de seguridad consiste en utilizar dispositivos dedicados, hardware solo utilizado como monedero, sin posibilidad de instalar otras aplicaciones potencialmente maliciosas.

Con respecto a las transacciones, se recomienda la opción de la multi-firma para aprobación de transacciones, la cual es una característica del cliente Bitcoin para garantizar que una transacción sea aceptada solo si es firmada por los miembros con posibilidad de aprobación de la misma.[32] También se recomienda usar un sistema para detectar transacciones inseguras en caso de no poder esperar por las confirmaciones de las transacciones instantáneas e incluso, las empresas con pagos recurrentes

[31] Monedero *offline, cold storage* o almacenamiento en frío: reserva de bitcoins que no está conectada a la red.

[32] Si la llave privada inicia con 1 implica el uso de solo una llave pero si inicia con 3, implica que se requiere múltiples llaves privadas para desbloquear un pago o transacción.

pueden ejecutar sus propios nodos para lograr rapidez en las verificaciones y una seguridad independiente [2].

Para el caso del nodo completo**,** se debe verificar que el dispositivo cumpla los requisitos necesarios del equipo, de la conexión, configuración de *firewall/ router* y buenas prácticas de seguridad[33] para evitar situaciones de riesgo. En todo caso, se debe proteger con una contraseña fuerte el fichero *bitcoin.conf* y solo abrir los puertos necesarios, al exterior.

Medidas de seguridad

Principalmente, se recomienda realizar periódicamente respaldos de todo el monedero (no solo de las claves privadas[34] de la direcciones), encriptar y mantener bien resguardada una versión en un medio físico (USB, CD, papel, etc.) para mayor seguridad. Asimismo, se debe tener especial cuidado con monederos en línea: poseer un respaldo encriptado, acceso con autenticación de dos factores y la protección necesaria contra malware en los equipos a utilizar.

Para mantener la privacidad, se recomienda no usar la misma dirección para varias transacciones, es mejor utilizar un par de claves nuevas para cada transacción y mantener las claves públicas anónimas [7].

El recurso humano es un punto fundamental a tomar en cuenta: se debe hacer negocios solo con personas u organizaciones conocidas, de confianza o con una buena reputación. Además, se recomienda a los comerciantes validar el costo/beneficio de aceptar pago rápidos (con cero o pocas confirmaciones por transacción) dada la posibilidad de que sean víctimas de un ataque.

Finalmente, no se deben obviar las medidas básicas de seguridad: instalar el cliente del software del Bitcoin desde repositorios o páginas oficiales verificadas, mantener las actualizaciones del software al día, mantener los equipos y monederos cifrados con contraseñas robustas, mantenerse informados sobre las novedades relativas al protocolo y la moneda en general.

[33] Estas características son definidas y recomendadas por Bitcoin.org

[34] Si se pierde la llave privada o la billetera, las BTC relativas a esos elementos se perderán para siempre.

3.1. Asociadas al uso de recursos de operación

Con respecto al uso de TOR y TAIL, como todo software o sistema operativo, estos cuentan con vulnerabilidades de seguridad que han sido corregidas con versiones recientes o que, por medio de amenazas relacionadas con fallos de aplicaciones complementarias a estos sistemas (por ejemplo fallos en *Firefox* con *TOR Browser Bundle*[35]) comprometen indirectamente el funcionamiento de estos sistemas. Por otro lado, en un estudio realizado por investigadores de la Universidad de Luxemburgo [17] se analiza la posibilidad de realizar un ataque *man-in-the-middle* explotando los mecanismos anti DDos de Bitcoin y el uso de TOR, de manera que el atacante puede ver toda la información de la víctima, conocer su dirección IP y comprometer su privacidad. Con este ataque, no obstante, no es posible el robo de monedas ni la modificación de ningún elemento del proceso.

Otro elemento a tomar en cuenta es la plataforma P2P, la cual puede ser utilizada para sobrepasar los cortafuegos (*firewalls*) y distribuir *malware*. De acuerdo al glosario de Malware de TechTarget, los *P2P Botnets* son redes de *bots* que si bien trabajan sin un servidor C&C[36] el *software* del *bot* maneja una lista de computadoras infectadas y de confianza, sitios de entrega de información y lugares donde las máquinas pueden actualizar su *malware*, lo que complica más detectar y rastrear las comunicaciones de estas redes y sus ataques. Asimismo, los procesos en línea, como cualquier proceso que implique conexión a internet, pueden verse expuesto a problemas como ataques *man in the middle*, *phishing, tabnabbing*[37], robo de sesiones, exposición de datos, etc., en caso de no contar con las medidas de seguridad en el equipo o la red.

Finalmente, los nodos completos y el puerto abierto que este requiere deben ser analizados, pues el mantener un puerto abierto es considerado un

[35] TOR integrado en el navegador Mozilla Firefox.
[36] C&C server: servidor command and control.
[37] *Tabnabbing:* tipo de *phishing*, emplea scripts para reemplazar la página legítima en una pestaña que no esté activa por una copia creada por el atacante.

riesgo de seguridad debido a que permite una excepción en el *firewall* que puede ser aprovechada por nodos maliciosos para propagar malware y obtener accesos indebidos a los equipos.

3.2 Herramientas

Los monederos electrónicos son la principal herramienta del protocolo, para el cual no solo existe el peligro de hackeo del mismo (sea en línea o no) sino también existe la posibilidad del mal uso del mismo por parte del usuario, quien puede revelar información sensible (claves privadas), no respaldar adecuadamente el monedero o no aplicar las medidas básicas de seguridad a los equipos donde lo instala.

A pesar de que actualmente solo existen pocos en el mundo, los cajeros automáticos de bitcoins conforman otra herramienta a tomar en cuenta. Estos poseen los mismos riesgos que cualquier equipo que dispense dinero: pueden ser objeto de vandalismo, robo, mala configuración, etc.

Por otro lado, el uso de códigos QR y tecnología NFC que se utilizan para enviar las direcciones, pueden ser fuente de fallos por incorrecta implementación del software o problemas en el sistema operativo del dispositivo, así como situaciones por comunicaciones inseguras y peligros correspondientes al equipo que alberga la información de esta tecnología. Sucede una situación similar con la instalación del cliente Bitcoin y sistemas operativos/softwares/App asociados al protocolo, pues como toda aplicación puede ser víctima de vulnerabilidades debido a una incorrecta implementación, configuración o programación del software o algún componente de este.

3.3 Inherentes al funcionamiento de Bitcoin

A pesar de ser una de las características esenciales del protocolo, las transacciones instantáneas son menos seguras pues estas son recibidas en poco tiempo sin la certeza de que estén confirmadas, por lo que son vulnerables a ataques. Se considera oficial el ingreso de la transacción al *block chain* luego de 6 confirmaciones, es decir, aproximadamente 1 hora

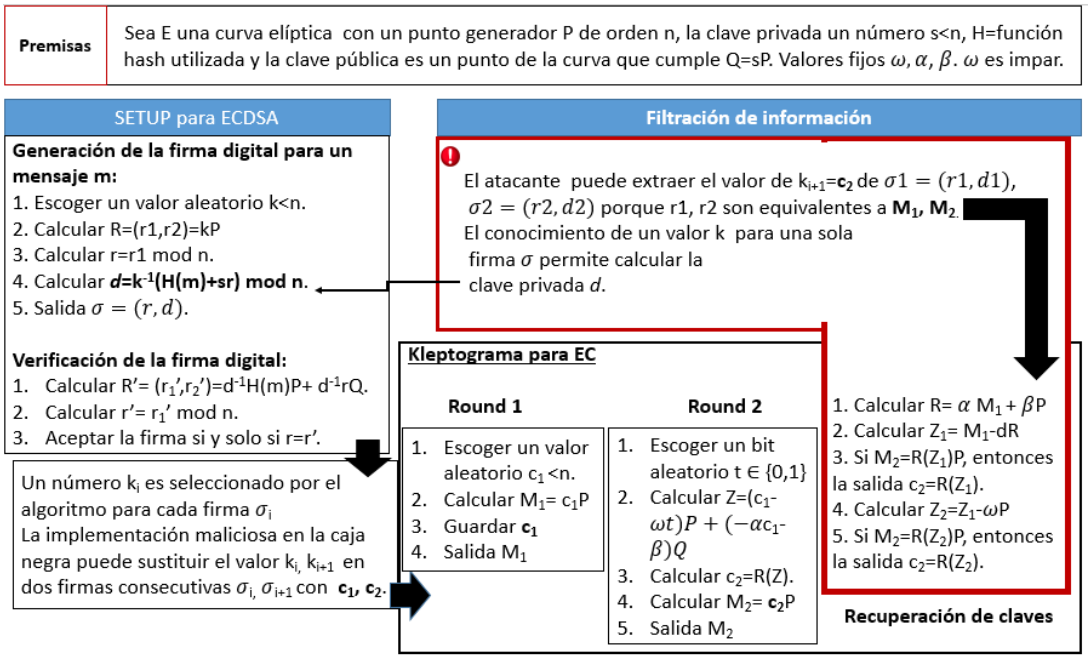
después de realizada la transacción (cada confirmación toma en promedio 10 minutos). Otra situación referente a este tema son las transacciones *spam*, pues dado que todas las transacciones son guardadas por todos los nodos, se genera un tráfico y un almacenamiento considerable[38]. Como solución, se han limitado las transacciones más problemáticas que son más difíciles de verificar y cuyo costo de operación resulta más caro que el valor de la transacción en sí, pues este sobrecargo puede provocar problemas de disponibilidad del servicio si continúa creciendo.

Por otro lado, algunos fundamentos criptográficos pueden ser potencialmente vulnerables a ataques. La función SHA256 es potencialmente vulnerable al ataque no lineal de rondas reducida y al ataque diferencial de orden superior, RIPEMD-160 al ataque diferencial y ambos casos pueden ser potencialmente vulnerados con ataques de pre-imagen y colisión [11]. Por otro lado, ECDSA puede ser potencialmente susceptible a las siguientes vulnerabilidades [11]: aleatoriedad insuficiente o pobre cuando se utiliza la misma clave pública para múltiples transacciones Bitcoin o el mismo par de claves y al ataque de curva inválida. Con respecto a la curva secp256k1, en caso de que la clave privada se encuentre cerca de uno de los 768 puntos de encuentro de la curva, está se considera débil y atacable. Cabe aclarar que esta amenaza existe solo en casos donde no se posea una fuente adecuada de aleatoriedad, pues el espacio alrededor de los puntos de encuentro es una fracción minúscula del espacio de claves total. Sin embargo, en el 2013 se detectó una vulnerabilidad con un componente para generar números aleatorios del sistema operativo Android, el cual debido a una mala programación provocó que las claves privadas generadas por las billeteras móviles de este sistema no fueran realmente aleatorias, una falla crítica aprovechada por los hackers hasta la actualización del sistema operativo.

Asimismo, existe un ataque a la criptografía basada en el logaritmo discreto desarrollado en el año 1997 y cuya actualización aplicada al ECDSA utilizado por Bitcoin fue descrita por Stephan Verbücheln en el 2015 [18]. Este

[38]El tamaño actual de la cadena de bloques es de 20Gb y para evitar la sobrecarga se mantiene un máximo de 1 MB por bloque.

es un ataque kleptográfico que utiliza un SETUP[39] en una implementación maliciosa de un criptosistema con especificaciones públicamente conocidas del tipo caja negra[40] donde el algoritmo criptográfico es alterado de manera que filtra información a través de la firma digital sin aplicar ningún ataque lateral y con posibilidad de ser computacionalmente indistinguible. El atacante, conocedor de la curva y el punto generador utilizado por la víctima, crea su propia billetera maliciosa e inicia operaciones con la billetera legítima de la víctima. Luego, el atacante vigila las transacciones en espera de dos transacciones consecutivas de la misma dirección y extrae la clave privada como se explica en la figura 12. Con este dato, puede gastar las monedas asignadas a esa dirección.



Fuente: Elaboración propia basado en información de [18]

Figura 12. Ataque kleptográfico al ECDSA aplicado a Bitcoin

Por otro lado, existe una mínima posibilidad de 'colisiones' en la creación de direcciones, es decir, que dos personas generen de forma independiente dos direcciones iguales. Si esto sucede, entonces tanto el propietario original de la dirección como el propietario que 'colisiona' podrían gastar el dinero enviado a esa dirección, pero no es posible que el propietario que 'colisiona' pueda gastar la billetera entera (o viceversa) del propietario

[39] SETUP o Secretly Embedded Trapdoor with Embedded Protection es un *exploit* que consiste en incrustar de manera secreta una trampa en un criptosistema.
[40] Caja negra se refiere a que se desconocen los procesos internos del programa.

original. Cabe resalta que toma 2 ^{107} veces más tiempo generar una colisión intencionada que generar un bloque, por lo que se considera que este ataque no es rentable.

También existen dudas por el uso de la curva secp256k1 en lugar de utilizar curvas totalmente rígidas[41] o con respecto al uso del codificado Base58 en lugar del Base64 (a pesar de que el autor del protocolo justifica su elección en este caso). De acuerdo con SafeCurves, si bien el proceso de generación de la curva secp256k1 no está completamente detallado, las partes no explicadas no dan a los generadores de la curva muchos bits de control, lo que no implica una amenaza de seguridad, pero mantiene la duda con respecto a la justificación de elección de los parámetros de esta curva.

Finalmente, las funciones hash y ECDSA no están exentas a problemas independientes del algoritmo matemático, como fallas en la implementación, ataques *side-channel* o de canal lateral, errores de *software*, defectos de diseño o programación de las funciones/algoritmos o de que sean quebradas cuando se logre construir una computadora cuántica práctica para atacar estos algoritmos [11].

Otra amenaza importante de señalar es la bifurcación de la cadena de bloques: Puede suceder que múltiples bloques tengan la misma altura del bloque (*block height*), como es común cuando dos o más mineros producen cada uno un bloque aproximadamente al mismo tiempo. Esto puede producir un *fork* o bifurcación en la cadena, pero los mineros deben adjuntar el bloque solo a uno de los extremos, el cual, por regla de consenso, debe ser la cadena con mayor dificultad de ser recreada.[42] Esta situación puede ser aprovechada por nodos maliciosos para realizar varios tipos de ataques o puede conllevar a problemas de distribución de información y pérdidas financieras.

Con respecto a los nodos maliciosos y nodos egoístas, el creador del protocolo Bitcoin aclara que toda la cadena de confianza se garantiza mientras la mayoría de los nodos sean honestos. Sobre este hecho se han

[41] Curva rígida: según SafeCurves, una curva rígida implica que se conoce complemente el proceso de generación de la curva.

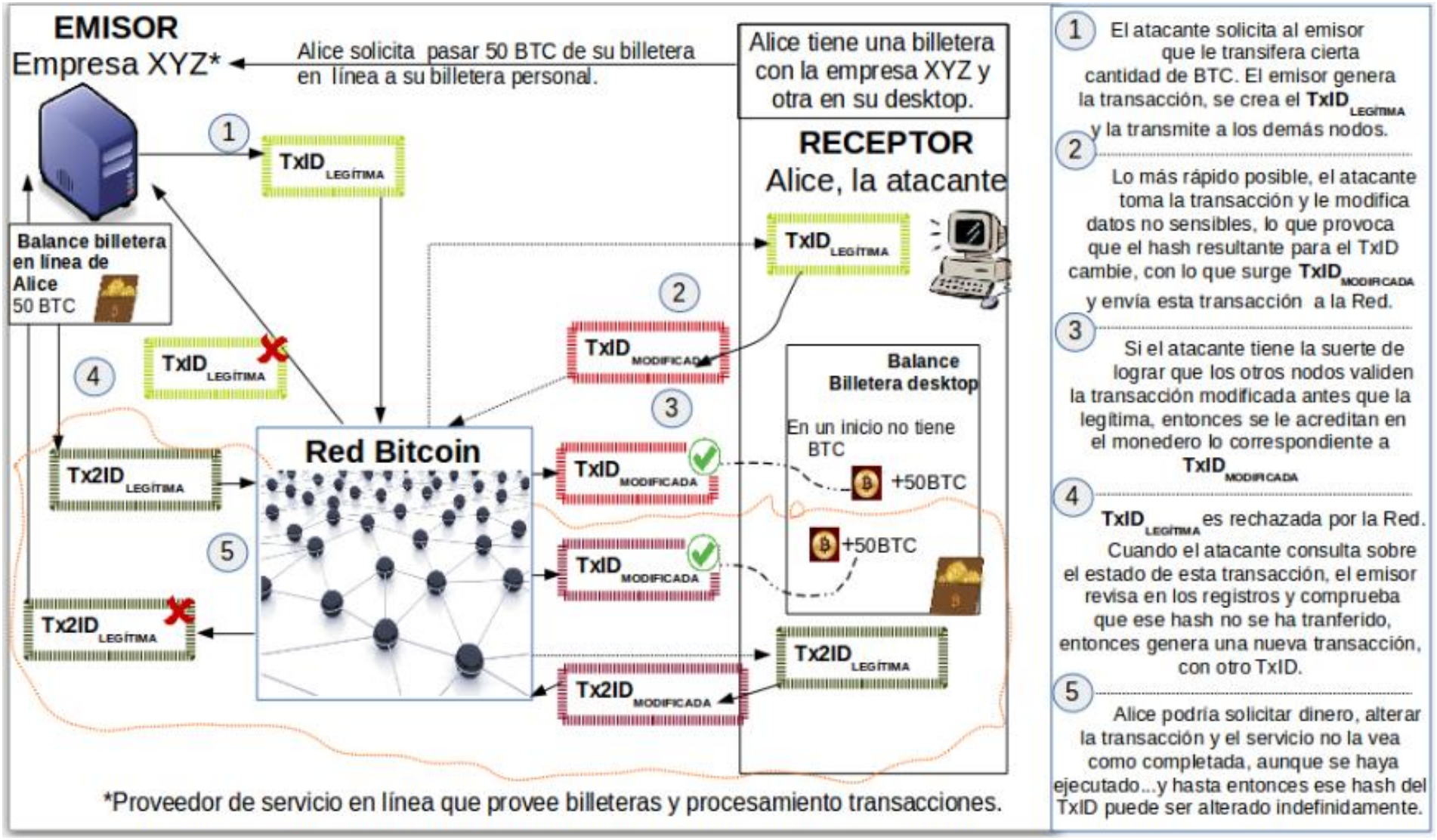
[42] Esto previene un ataque donde alguien bifurque la cadena a propósito para crear una gran cantidad de bloques de baja dificultad que sea la más larga en longitud. A fin de evitar esta ambigüedad, se aclara con la regla de consenso que la expresión “más larga” se refiere a dificultad y no a cantidad de bloques.

realizado varias investigaciones para determinar si con el 50% o porcentajes menores del poder computacional de la red es posible realizar cambios prohibidos[43] los cuales dada la naturaleza del protocolo, quedarían registrados permanentemente. Por ejemplo, una investigación de la Universidad de Cornell demostró que, teóricamente, con un 25% de poder sobre la red, es posible retrasar las transacciones, anular los esfuerzos del resto de mineros para asegurar la red y demostrar que el modelo de incentivos no es suficiente para evitar ataques por *pooles* de nodos egoístas [19].

El ataque del *pool* de nodos egoístas se basa en la posibilidad de que mineros maliciosos puedan bifurcar el *block chain*, crear una cadena privada para generar y ocultar bloques durante largos periodos de tiempo, para luego liberar juiciosamente esos bloques, de manera que obligan a nodos honestos a abandonar la rama pública legítima de la cadena y a usar su capacidad computacional en esos bloques que están destinados a no formar parte de la *block chain.* De este modo, permite al pool de nodos egoístas recolectar mayores ingresos mediante la incorporación de una mayor fracción de sus bloques en el *block chain*. Con este aumento de ganancias puede atraer a nodos honestos al *pool* egoísta y este adquiere mayoría, con las consecuencias que esto implica para el protocolo y su cadena de confianza. Sin embargo, se considera estadísticamente imposible este ataque pues mientras los mineros maliciosos esconden unos bloques, otros mineros honestos descubrirán dichos bloques, los registrarán en el *block chain* y dado que es prácticamente imposible cambiar el historial de bloques, se evidencia la modificación y el ataque [20].

Por otro lado, una vulnerabilidad famosa fue la maleabilidad de transacciones: era un fallo en la implementación[44] del cliente Bitcoin que permitía la alteración de los detalles de la transacción sin alterar la firma digital y propiciaba el doble gasto [10] [21]. En la Figura 11 se detalla el ataque paso a paso para su mejor comprensión.

[43]Excluir, modificar y revertir transacciones, superar las 6 confirmaciones necesarias o generar un *fork* en la cadena bloques y lograr que sea considerado como el más largo, dado que puede construir bloques más rápido que el resto de la red [11].
[44] Casos conocidos ocurrieron en servicios de cartera y procesamiento de transacciones. Mt.Gox, Bitstamp, hasta Silk Road sufrieron este ataque [21].



Fuente: Elaboración propia basado en información de [10] [21]

Figura 13. Funcionamiento del ataque de maleabilidad de transacciones

Existen varias maneras de modificar los datos en la TxID pero estas técnicas no se detallarán, pues lo importante es recalcar que un cambio mínimo en un campo de un elemento de la transacción lograba cambiar el hash y por ende el TxID sin romper la firma digital [10]. El tema se solucionó con un parche[45] que incluye la verificación del formato de la transacción estándar.

Finalmente, existen otros ataques referentes al doble gasto, los cuales son un riesgo para los pagos rápidos o transacciones instantáneas sin confirmaciones[46]. Cabe resaltar que en estos ataques influye la posible intervención en las comunicaciones, donde el atacante puede tener nodos cómplices cercanos al radio que ayuden a distribuir con mayor rapidez la Tx y delegar la Tx Falsa [9]. Entre estos ataque se encuentra el *Race attack* y el ataque *Finney*,[47] el cual es un poco más complicado y con un costo mayor al anterior (si el atacante falla, pierde la recompensa del bloque) pero para tener una mayor posibilidad de éxito, el atacante debe tener un *hashrate* considerable, ser minero y controlar el contenido de sus bloques [22].

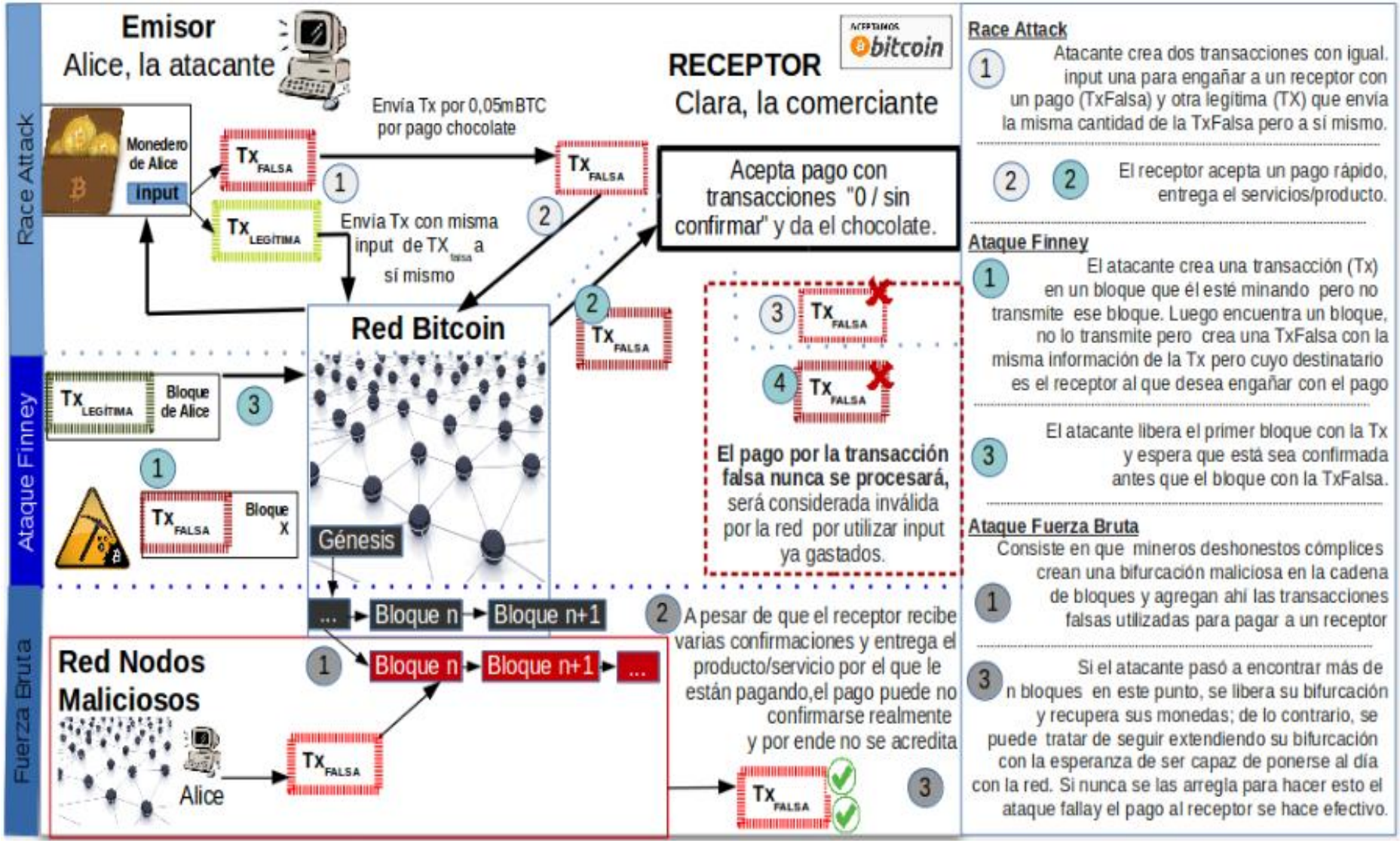
Otro caso es el Ataque Vector76, conocido como un ataque de 1 confirmación, el cual es una combinación del *Race* attack y el ataque *Finney* y finalmente el clásico ataque de Fuerza Bruta, donde se requiere que el atacante posea mayoría en la red pero no limita el ataque a que el receptor espere por confirmaciones [9].

En la Figura 13 se muestra un esquema con el detalle de los ataques *Race*, *Finney* y de Fuerza Bruta para su mayor comprensión.

[45] A pesar de que se entiende que es un problema de la implementación del software y no del protocolo en sí.

[46] Necesarias para casos de ventas o servicios que requieren un cobro rápido, como máquinas expendedoras, supermercados, etc.

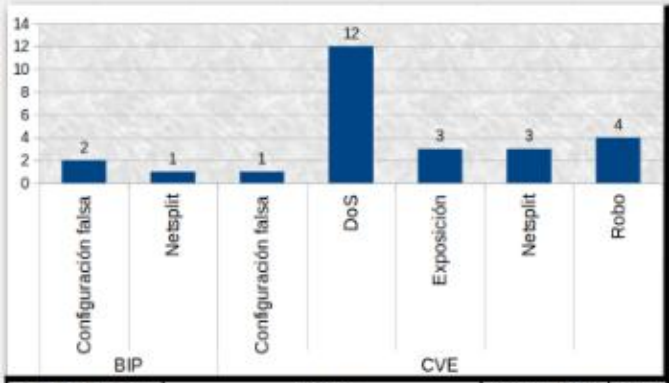
[47] Este ataque es famosos porque se utilizó contra el sitio de apuestas SatoshiDice.



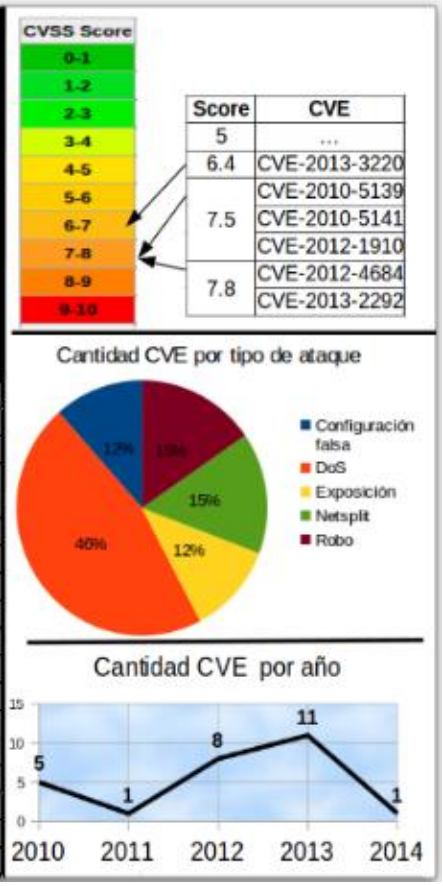
Fuente: Elaboración propia basado en información de [9] [22]

Figura 14. Diagrama de ataques de doble gastos

Finalmente, los fallos de seguridad y *Common Vulnerabilities* and *Exposures*[48] (CVE) recopilados en el wiki de Bitcoin (23 CVE y 3 BIP-*Bitcoin Improvement Proposal*[49]**)** y en el sitio *CVE Detail* (22 ya enlistadas en el wiki) es una fuente de información valiosa para determinar los puntos críticos de fallo del modelo. Con estos datos, se realiza un breve análisis para determinar las vulnerabilidades de seguridad encontradas (y corregidas) hasta el momento, datos que se sintetizan en la Figura 14.



Tipo ataque	Afecta	Severidad	CVE
Configuración falsa	All Bitcoin clients	Mineros	2
	bitcoind and Bitcoin-Qt 0.8.0	Mineros	1
DoS	bitcoind and Bitcoin-Qt	Difícil	1
		Fácil	6
	bitcoind and Bitcoin-Qt 0.8.x	Fácil	1
	bitcoind & Bitcoin-Qt for Windows	Difícil	1
	wxBitcoin and bitcoind	Fácil	3
Exposición	bitcoind and Bitcoin-Qt	Fácil	2
	wxBitcoin and bitcoind	Difícil	1
Netsplit	All Bitcoin clients	Implícito	1
	Bitcoin protocol and all clients	Muy Difícil	1
	bitcoind and Bitcoin-Qt	Difícil	1
		Fácil	1
Robo	bitcoind and Bitcoin-Qt	Local	1
	Anything using OpenSSL for TLS	Fácil	1
	wxBitcoin and bitcoind	Fácil	2
Total Result			26



Fuente: Elaboración propia con información de Wiki Bitcoin y CVE Details

Figura 15. Información sobre vulnerabilidades reportadas en el protocolo.

La mayoría de vulnerabilidades propician ataques de denegación de servicio (46%) seguido por los ataque que involucran robos de criptomonedas y ataques *netsplits* (el atacante puede crear varias vistas de la red, permitiendo doble gasto con más de 1 confirmación). De la Figura 14 se

[48] Los datos de vulnerabilidades CVE se toman de la base de datos de vulnerabilidades nacionales proporcionado por el National Institute of Standards and Technology-NIST.
[49] Una Propuesta de Mejoramiento de Bitcoin (BIP) es un documento de diseño para la introducción de características o información para Bitcoin.

resaltan los CVE con mayor puntuación[50] a fin de profundizar en los casos más importantes y se enlistan en la Tabla 2.

Tabla 2. Vulnerabilidades en el protocolo Bitcoin con mayor puntuación

Score	CVE	Afecta	Tipo ataque	Ataque es...	Falla	Consecuencia
7.8	CVE-2013-2292	bitcoind and Bitcoin-Qt	DoS	Difícil	Una transacción que toma por lo menos 3 minutos para verificar	Permite a atacantes remotos provocar una denegación de servicio por la minería en un bloque para crear una transacción Bitcoin no estándar que contiene múltiples códigos de operación de script OP_CHECKSIG.
7.8	CVE-2012-4684	bitcoind and Bitcoin-Qt	DoS	Fácil	La funcionalidad de alerta en es compatible con diferentes representaciones de caracteres de los mismos datos de la firma, pero se basa en un hash de esta firma.	Permite a atacantes remotos provocar una denegación de servicio a través de una válida firma modificada para una alerta de circulación.
7.5	CVE-2012-1910	bitcoind & Bitcoin-Qt for Windows	DoS	Difícil	No uso MinGW manejo de excepciones-multi-hilo de seguridad (*MingW multithreading*)	Permite a atacantes remotos provocar una denegación de servicio o posiblemente ejecutar código arbitrario a través de mensajes de protocolo Bitcoin artesanales.
7.5	CVE-2010-5141	wxBitcoin and bitcoind	Robo	Fácil	Control incorrecto de los códigos de operación de script en las transacciones Bitcoin.	Permitía a atacantes remotos pasar bitcoins de otros usuarios a través de vectores no especificados.
7.5	CVE-2010-5139	wxBitcoin and bitcoind	Robo	Fácil	Desbordamiento de integer (overflow de outputs) coordinado.	Permite a atacantes remotos evitar las restricciones económicas previstas y crear muchos bitcoins a través de una transacción de Bitcoin diseñado.
6.4	CVE-2013-3220	bitcoind and Bitcoin-Qt	Netsplit	Difícil	No consideran adecuadamente si el tamaño de un bloque podría requerir un número excesivo de bloqueos de base de datos.	Permite a atacantes remotos provocar una denegación de servicio y permiten ciertas capacidades doble de gasto a través de un gran bloque que desencadena incorrecta bloqueo Berkeley DB.

Fuente: Elaboración propia con información de Wiki Bitcoin y CVE *Details*

Con la información presentada se puede concluir que los elementos más atacados son el bitcoind, Bitcoin-Qt y wxBitcoin (versiones del cliente Bitcoin) y los ataques con mayor impacto/cantidad son aquellos de DoS.

Es importante destacar que la mayoría de las debilidades del protocolo ya están definidas y enlistadas dentro del wiki de Bitcoin, por lo que es fundamental informarse de estas posibles vulnerabilidades antes de incursionar en el uso del protocolo y la criptodivisa.

[50] *Common Vulnerability Scoring System*, CVSS, es un sistema de puntuación de vulnerabilidades diseñado para proporcionar un método abierto y estandarizado para clasificar vulnerabilidades de TI.

3.4 Fraudes y otros ataques

Las casas de intercambios de bitcoins y servicios en línea han sido blanco de varios ataques que han manchado la imagen del protocolo. El caso más importante es Mr.Gox, plataforma de intercambio de criptodivisas que en el 2014 se declaró en quiebra luego de múltiples fallos de seguridad e inestabilidad financiera. Esta casa de cambio, la cual en su momento contó con 1 millón de clientes y manejaba el 70% de las transacciones en la red BTC, sufrió varios ataque desde su creación en el 2010 [7]. Otros casos similares han sucedido con Flexcoin (quiebra por hackeo) y BTER, quien denunció un robo de 7,170 bitcoins a billeteras en almacenamiento frío [21] [23].

Otro ataque conocido es el caso del monedero falso (*fake-wallet attack*), para el cual si bien no existen registros de ataques en Bitcoin, es posible su realización por la simpleza de ejecución del mismo. Este consiste en repartir software falso de los monederos en distintos medios (foros, blogs, etc.), el cual instala *keyloggers* que roban contraseñas y busca cualquier archivo *wallet.dat* de la criptodivisa para luego enviarlo a un servidor remoto del atacante.

Por otro lado, existen varios casos de estafas asociados a las Bitcoin, desde casa de cambio fantasmas o mercados en línea que sufren “pérdidas” de BTC, hasta compañías virtuales con softwares de minería de criptomonedas con posibilidades de pago vía PayPal (por ejemplo *Coingeneration, IPU Services)* pero cuyos colaboradores nunca reciben el pago o son víctimas de otros engaños como la utilización del procesamiento para otros propósitos, infección de equipos, etc.

En el caso de ataques directos y malware, en los últimos años se han surgido diversos métodos para lograr infectar equipos con el fin de “robar” ciclos de procesamiento del CPU para la minería o directamente criptodivisas de los monederos. Por ejemplo:

- Extensiones maliciosas de browser (ejemplo BTC-E BTC, *Cryptsy Dogecoin Live Ticker*, entre otras), donde el software dentro de la

extensión monitorea la actividad web de los usuarios, presta atención a las visitas a sitios de intercambio de criptodivisas (como *Coinbase*, *MintPal*) y cuando el usuario realiza una transacción, la extensión maliciosa sustituye a la dirección de recepción con una dirección de BTC diferente de su propia (dirección bitcoin del atacante) [24].

- Ataques DDoS a *pooles* de mineros o casas de cambio: el conocido ataque de denegación de servicio ha sido utilizado para atacar a grandes *pooles* de mineros, quienes han visto afectadas sus operaciones y reciben extorsiones de pago en BTC para detener los ataques [25].

- Actualizaciones del cliente P2P de *uTorrent* , el cual da la opción de instalación del software *Epic Scale*, el cual permite la utilización de ciclos de procesamiento libres para simulaciones físicas, minería de criptodivisas, entre otras funciones.

- Nueva familia de malware para dispositivos móviles llamados *Cryptominers/Coinkrypt*. Este tipo de malware, en su mayoría troyanos y cuando se instala, secuestra el dispositivo para silenciosamente minar criptodivisas para el autor del malware. Aparte de cualquier gasto de dato incurrido, el uso constante de hardware del dispositivo también puede afectar la vida de la batería y vida útil del equipo. También existen versiones de estos malware que se dedican a robar bitcoins directamente de las billeteras. Ejemplos*: el botnet Kelihos*, los troyanos ZeroAccess y Mac [20].

- Abuso del *block chain*: el Laboratorio Kaspersky en conjunto con la Interpol advirtieron sobre la posibilidad del abuso de la cadena de bloque para inyectar malware o material de pornografía infantil y almacenarlo/ distribuirlo de manera permanente en este medio, el cual actualmente carece de métodos para eliminar datos de los bloques ya encadenados [20].

Capítulo 4: Situación legal y comercial

4.1 Nivel regulatorio

En Argentina, se considera que no es necesaria una legislación dedicada, pues la posición de las criptomonedas no contradice la ley vigente y pueden utilizarse las herramientas legales disponibles para atender casos relacionados con las BTC, según la opinión de Andrés Chomczyk, abogado especialista en el tema [26]. Sin embargo, el Banco Central de la República de Argentina se pronunció oficialmente sobre los riesgos del uso de criptomonedas y recalcó que no tienen curso legal ni poseen respaldo alguno debido a que no son emitidas por ellos ni por ningún estado extranjero, que no existen mecanismos gubernamentales que garanticen su valor oficial y los riesgos asociados son soportados exclusivamente por los usuarios de las mismas [27].

El principal temor de las entidades gubernamentales es el uso de estas para lavado de activos y financiación de actos terroristas. Cabe resaltar que mientras un Banco u otro sujeto obligado no esté relacionado con la transacción, los entes reguladores de impuestos y verificación de operaciones sospechosas no pueden intervenir en las transacciones. Finalmente, no se espera ningún tipo de pronunciación oficial más allá de las ya emitidas (comunicado oficial del BCRA, resolución UIF 300/2014[51]) [27].

El panorama en Costa Rica es similar pero sin pronunciaciones formales por parte de los entes financieros oficiales Un estudio realizado por el abogado Julio Córdoba resalta varios puntos de las criptodivisas con respecto a la legislación costarricense vigente: si bien no existe una normativa específica para monedas electrónicas ni criptomonedas, si la moneda es minada fuera del país, no contradice el monopolio de emisión de dinero del Banco Central de Costa Rica, por lo que puede ser utilizada por el público en general y estas deben recibir el tratamiento jurídico de las

[51] Resolución UIF 300/2014.Prevención del lavado de activos y de la financiación del terrorismo, reporte de operaciones efectuadas con monedas virtuales.

monedas internacionales, el cual incluye protección legal en caso de delito [6].

4.2. Aceptación y uso comercial

A nivel general, a una sociedad como la argentina y la venezolana le resulta beneficioso el uso de Bitcoin como reserva de valor frente a la depreciación de su moneda y las estrictas políticas con respecto a las monedas extranjeras. Su utilización se está extendiendo, más comercios y usuarios son adeptos a la filosofía gracias a las exposiciones y reuniones organizadas por la rama de la comunidad local Bitcoin llamada ONG Bitcoin Argentina[52], quienes organizan varias actividades para la divulgación de información con respecto a este tema. Cabe resaltar, que Argentina se ubica actualmente en la posición 30 a nivel mundial de los países que más utilizan BTC (a nivel latinoamericano solo es aventajado por Brasil) y su nivel de penetración del internet (68%) hace terreno apto para la incursión y desarrollo de esta tendencia [28].

Por su parte, Costa Rica posee una economía un poco más estable, con una moneda poco fluctuante y libre comercio de capitales[53], razón por la que la sociedad costarricense posee menor interés de recurrir a este recurso. No obstante, el turismo es una fuente importante de divisas al país, por lo que la no incorporación al mundo bitcoin puede repercutir en pérdida de clientes. Sin embargo, después del escándalo con *Liberty Reserve*[54] y el reciente pago de un secuestro con Bitcoins, el tema quedó empañado pues se asocia con el posible incremento de actividades delictivas o ilícitas. Aunado a estas circunstancias, la falta de grupos de divulgación, charlas informativas y comunidades consolidadas de Bitcoin agravan el escepticismo alrededor de las criptomonedas.

[52] Antes conocida como Fundación Bitcoin Argentina.

[53] Sin embargo, esta situación no limita el interés de las bitcoins en una sociedad similar. Por ejemplo, Australia es un estado con mejores condiciones que Costa Rica y es un gran entusiasta de Bitcoin y las altcoin.

[54] Una casa de cambio de divisa privado con sede en el país pero de capital estadounidense con su propia moneda digital cerrada por lavado de dinero.

Capítulo 5: Análisis

5.1 Ventajas y Desventajas

La principal ventaja de este protocolo es aportar un ambiente confiable a una comunidad deseosa de libertad de comercio. Los usos que los participantes le han dado a esta criptodivisa van desde envío de remesas por parte de inmigrantes africanos a un costo 4 veces menor[55] hasta donaciones anónimas a organizaciones como *Wikileaks*. Así mismo, la comunidad de participantes de esta filosofía ha creado todo un nicho de mercado alrededor de la criptomoneda: apps especializadas, servicios asociados, inclusive aplicaciones ociosas como *SatoshiDice*, recursos que se basan en la confiabilidad otorgada por la robustez criptográfica del protocolo y la red.

Sin embargo, investigaciones académicas han refutado algunas características representativas de Bitcoin. Por ejemplo la privacidad asociada con el uso de Bitcoin, ha sido desestimada por varias investigaciones académicas, pues es posible realizar un análisis estadístico (independientemente del uso de TOR o mezcla de direcciones) de todos los registros públicos en la cadena de bloques para hacer un rastreo de cuentas [7] e inclusive determinar la dirección IP del emisor [17] bajo ciertas situaciones.

Por otro lado, con respecto al tema financiero, este esquema ha sido calificado de Esquema Ponzi, burbuja financiera, etc. Así lo definió el reconocido economista Nouriel Roubini quien criticó la posición de las criptodivisas debido a la volatilidad, usos ilegales y falta de protección en caso de robo [29].

Finalmente, las criptodivisas ganaron notoriedad por razones poco agradables: son utilizadas para pagos de servicios/productos donde la gente normalmente no desea utilizar la tarjeta de crédito o ligar su identidad. Por tal razón, muchos relacionan las monedas con mercados clandestinos en línea (como *Silk Road*) o solicitudes de pago por *ransomware* o extorsiones.

[55] Comparado con medios convencionales de envío de dinero.

5.2. Retos

Uno de los mayores retos que debe sobrellevar este protocolo es la especulación, pues la filosofía de libertad de comercio de las criptomonedas se ve empañada por los usuarios que no siguen esta idea, las guardan y no las colocan en circulación. Por lo tanto, la comunidad Bitcoin debe incentivar el uso de la moneda como un medio real de intercambio comercial más que como una herramienta de inversión.

Asimismo, la prevención del uso de bitcoins en actos de lavado de activos, financiación de terrorismo y comercio de material ilícito es un reto fundamental para lograr mejorar su reputación. Para mitigar esta problemática, una opción es desarrollar filtros detectores de comportamientos sospechosos, que puedan ser añadidos como parte de las reglas de consenso de la red y generen alertas para mitigar esta problemática. Una situación similar sucede con las casas de intercambio por los múltiples casos de hackeo y bancarrota. Por esta razón, algunos países han tomado cartas en el asunto (por ejemplo Singapur) pero la auditoría o regulación de estos entes debería ser una meta para la comunidad Bitcoin, debido a que por problemas de terceras partes, la aceptación de la moneda se ha visto afectada.

Por último, una limitante para la expansión del uso de bitcoins en la región es el acceso a la red, pues se estima que solo el 43% de Latinoamérica tienen acceso al internet [28].

5.3. Iniciativas

A partir del modelo de Bitcoin, algunas empresas y países se han interesado por el esquema de la cadena de bloques para crear un sistema de dinero digital pero controlado por los bancos centrales y con posibilidad de rastreo de los usuarios[56]. Además, existen otras iniciativas que buscan aprovechar este esquema para mantener registros de datos de manera segura, transparente, distribuida, con privacidad y en tiempo real, como el

[56] Se especula que IBM está desarrollando un proyecto de este tipo [30].

nuevo sistema propuesto por Factom que permite crear bases de datos sobre la cadena de bloque.

En cuanto a iniciativas con respecto al desarrollo y evolución del protocolo, se resaltan dos casos: el uso de *Proof-of-stake*, el cual es una prueba de participación que está basada en la edad de la moneda,[57] cuya implementación propone garantizar mayor seguridad y eficiencia energética. Actualmente se utiliza en *PeerCoin* de manera híbrida con POW. El otro caso es la segunda generación de criptodivisas, la cual pretende corregir los fallos de sus predecesoras y añadir las actualizaciones en fundamentos criptográficos como la aplicación de hashcash-SHA3, posible uso de una curva elíptica con mejores condiciones de seguridad y eficiencia computacional como E-222, Curve25519, etc. y aplicar los nuevos métodos criptográficos adecuados para las computadoras cuánticas.

[57] Edad de la moneda: número de monedas que se tienen en un periodo, se calcula mediante la marca de tiempo *(timestamp*) de cada transacción en los bloques. En Bitcoin, se utiliza para priorizar las transacciones.

Conclusiones

A partir de la información recolectada y analizada en este trabajo, es posible determinar que, para un ciudadano común, incursionar en el mundo Bitcoin es una tarea difícil pues debe comprender cabalmente los métodos de funcionamiento y peligros asociados con la implementación y uso de este protocolo (tanto si es usuario como un comerciante anuente a aceptar este método de pago). Además, los últimos casos de problemas con intermediarios, aunado a la indefinición legal del estatuto de este tipo de moneda en varios países, no ayudan a demostrar la solidez necesaria para la incorporación generalizada de esta criptomoneda en la sociedad actual. Sin embargo, este es el proceder típico de toda nueva tecnología: en un inicio pocos entienden los mecanismos de funcionamiento, existen situaciones desfavorables con terceros que empañan el panorama y las leyes vigentes están desactualizadas con las nuevas tendencias. A pesar de ser una idea que viene gestionándose desde hace décadas[58], Bitcoin solo tiene 6 años de existencia, por lo que se puede considerar que este comportamiento es esperado y conforme se desarrolle y expanda su uso, es posible que la situación se normalice.

Por otro lado, se puede concluir que las bases criptográficas del protocolo son sólidas mientras las primitivas utilizadas estén vigentes, razón por la cual en conjunto con la infraestructura, implementación de medidas de seguridad adecuadas y los elementos humanos de confianza, el protocolo sí garantiza un medio para transacciones globales descentralizadas en relativamente poco tiempo, a bajo costo y de manera segura. Asimismo, se determina que en definitiva el eslabón débil de Bitcoin es el recurso humano, tanto los operadores de servicios (*pools* y casas de cambio) como los usuarios desinformados o descuidados.

Finalmente se resalta que esta criptodivisa no solo abrió un medio para el libre intercambio comercial, sino que también introdujo la idea de la cadena de bloques, cuyo uso se está expandiendo a otros ámbitos y fines, tema interesante para investigaciones futuras.

[58] Se toma como embriones de la idea los papers de Chaum (1982, Blind signature for payments), el de Dai (1998,B-money) y Law et al (1996, How to make a mint: the cryptography of anonymous electronic cash).

Glosario

ASIC: *application-specific integrated circuit* o circuito integrado para aplicaciones específicas. Es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general. Se usan para una función específica.

Backdoors o **puertas traseras:** *software* diseñado para abrir una vía de acceso a un sistema y permitir el control del mismo por parte del creador del programa.

Checksum: suma de verificación o suma de chequeo, es una función hash utilizada para validar la integridad de los datos al comprobar que no existan diferencias entre los valores iniciales y finales tras la transmisión.

Computacionalmente indistinguible: cuando la salida de un sistema alterado no se distingue mediante cálculo alguno de la salida de un sistema no modificado.

Criptodivisa: criptomoneda, del inglés *cryptocurrencies*, es un medio digital de intercambio, una divisas o moneda que utiliza primitivas criptográficas.

Distributed denial of Service **(DDoS/Dos):** ataque de denegación de servicio, es un ataque a un sistema de computadoras o red que provoca que un servicio o recurso sea inaccesible a los usuarios legítimos.

Exploit: es una parte de software, un fragmento de datos o una secuencia de comandos que se aprovecha de un error o vulnerabilidad con el fin de provocar un comportamiento no deseado o imprevisto en un software o hardware.

FPGA: *field-programmable gate array* o matriz de puertas programables. Es un dispositivo semiconductor que contiene bloques de lógica cuya

interconexión y funcionalidad puede ser configurada ‘in situ’ mediante un lenguaje de descripción especializado.

Hash: función hash, son algoritmos determinísticos que a partir de una entrada (una contraseña, un archivo, etc. de cualquier longitud) genera una salida alfanumérica de longitud fija que representa un resumen de toda la información ingresada como entrada, cadena que solo puede volverse a crear con esos mismos datos.

Keyloggers: software o software para guardar las pulsaciones en el teclado, información que luego se envía al atacante.

Kleptografía: uso de los canales subliminales y modificación de un sistema o un protocolo criptográfico de manera indetectable para lograr la fuga imperceptible de la información necesaria para la posterior recuperación de la clave privada.

Man-in-the-middle attack: cuando un atacante interfiere en las comunicaciones entre dos partes y accede a la información privada de estas.

Merkle tree: es un árbol de hashes donde los hashes de las transferencias se emparejan en forma de árbol binario (cada nodo tiene dos hijos), de manera que, cuando no se requieran dos hermanos (dos nodos que comparten el mismo padre), es posible eliminarlos y quedarse solo con el nodo padre sin perder la posibilidad de verificar el resto de nodos del árbol.

Método GVL -Gallant, Lambert and Vanstone: es un algoritmo muy eficiente para calcular el producto escalar en curvas de Koblitz, es decir poder calcular Q = kP en curvas elípticas que tienen endomorfismos eficientemente computables no triviales.

***Phishing*:** intento ilegal de adquirir información confidencial por parte de un atacante al hacerse pasar por una entidad de confianza en una comunicación electrónica.

Ramsonware: tipo de *malware* que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.

Side-channel attack: en términos criptográficos, se refiere a cualquier ataque basado en la información obtenida de la implementación física de un sistema de encriptación.

Timestamp: Marca temporal, marca de tiempo, registro de tiempo.

Anexos

Anexo 1: Cálculo de la probabilidad de éxito para el escenario de nodos maliciosos que generan una cadena alternativa [2].

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10    z=5
q=0.15    z=8
q=0.20    z=11
q=0.25    z=15
q=0.30    z=24
q=0.35    z=41
q=0.40    z=89
q=0.45    z=340
```

Bibliografía Específica

[1] Wong, J. Goldman Sachs Report Says Bitcoin Could Shape 'Future of Finance'. Coindesk. http://www.coindesk.com/goldman-sachs-report-says-bitcoin-could-shape-future-of-finance/ (consultado 11 marzo 2015).

[2] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash systema, 2008. https://bitcoin.org/bitcoin.pdf (consultado 26 agosto 2014).

[3] Serrano, S. La salud de Bitcoin: buen presente y mejor pronóstico. http://www.canal-ar.com.ar/21150-La-salud-de-Bitcoin-buen-presente-y-mejor-pronostico.html?pais=1 (consultado 20 marzo 2015).

[4] Vega, D. Bitcoin vs. Litecoin vs. Peercoin vs. Ripple vs. Namecoin. Heavy.com. http://heavy.com/tech/2013/12/bitcoin-vs-litecoin-peercoin-ripple-namecoin/ (consultado 30 marzo 2015).

[5] Faride, R. 2012. Black Hat.Is bitcoin an invitation for money laundering? http://www.riazfaride.com/black-hat/is-bitcoin-an-invitation-for-money-laundering/ (consultado 3 abril 2015).

[6]Córdoba, J.Bitcoin, criptomonedas y legislación en Costa Rica. https://prezi.com/-zqexyffwjni/bitcoin-criptomonedas-y-legislacion-en-costa-rica/ (consultado 6 abril 2015).

[7]Ron, D and Shamir,A. Quantitative Analysis of the Full Bitcoin Transaction Graph. http://ifca.ai/fc13/proc/1-1.pdf (consultado 15 agosto 2014).

[8] Apesteguia, E. La experiencia Bitcoin en la Argentina desde adentro. Infotechnology.comhttp://m.infotechnology.com/mobile/nota.html?nota=/contenidos/2013/10/29/noticia_0004.html (consultado 3 abril 2015).

[9] Karame, G. Androulaki, E and Capkun,S. 2012. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. https://eprint.iacr.org/2012/248.pdf (consultado 3 abril 2015).

[10] Chechik, D. Hayak, B. and Chechik, O. 2014. Black Hat 2014. Bitcoin Transaction Malleability Theory in Practice.https://www.youtube.com/watch?v=bmxu3r_CUKE&index=1&list=TLoxbTY1O89nk (consultado 2 marzo 2015).

[11] Yogesh,M. Bitcoin Protocol: Model of ‘Cryptographic Proof’ Based Global Crypto-Currency & Electronic Payments System http://yogeshmalhotra.com/BitcoinProtocol.html (consultado 3 abril 2015).

[12]Shirriff, K. Bitcoins the hard way: Using the raw Bitcoin protocol. http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html (consultado 3 abril 2015).

[13] Payeras, M. Isern, A. Puigserver, M. 2014.Introduccion a Bitcoin. Aula Virtual de Criptografía y Seguridad de la Información Cripto4you. Universidad Politécnica de Madrid. http://www.criptored.upm.es/crypt4you/temas/sistemaspago/leccion3/leccion03.html (consultado 3 abril 2015).

[14] Hecht, P. Clase de Criptografía II. Maestría de Seguridad Informática. Universidad de Buenos Aires.

[15] Longa, P. Sica. F. 2011. Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication. https://eprint.iacr.org/2011/608.pdf (consultado 3 abril 2015).

[16] Kristiján,G. 2014. Receiving Bitcoin. http://gisli.hamstur.is/2014/10/receiving-bitcoins/ (consultado 3 abril 2015).

[17] Biryukov,A and Pustogarov, I. 2015. Bitcoin over Tor isn't a good idea. Universidad de Luxemburgo. http://arxiv.org/pdf/1410.6079v2.pdf (consultado 3 abril 2015).

[18] Verbücheln, S. How Perfect Offline Wallets Can Still Leak Bitcoin Private Keys. https://www2.informatik.hu-berlin.de/~verbuech/klepto-ecdsa/klepto-ecdsa.pdf (consultado 30 mayo 2015).

[19] Eyal, I and Gun Sirer, E. 2014. Majority is not Enough: Bitcoin Mining is Vulnerable. http://ifca.ai/fc14/papers/fc14_submission_82.pdf. (consultado 15 agosto 2014).

[20] Donohue,B. Kaspersky Lab. 2013. El negocio de las bitcoins. http://blog.kaspersky.es/el-negocio-de-los-bitcoins/1867/ (consultado 3 abril 2015).

[21] Mateos, M. 2014. Maleabilidad de transacciones. http://www.genbeta.com/actualidad/por-que-mtgox-y-bitstamp-tuvieron-que-restringir-la-retirada-de-dinero (consultado 15 febrero 2014).

[22] Rosenfeld, M. What is a finney attack. http://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack (consultado 3 abril 2015).

[23] Higgins, S.BTER Claims $1.75 Million in Bitcoin Stolen in Cold Wallet Hack. http://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/ (consultado 10 marzo 2015).

[24] Cawrey, D. 2014. Chrome Extension Could Be Vulnerable to Cryptocurrency Malware. http://www.coindesk.com/chrome-extension-could-vulnerable-malware/ (consultado 3 abril 2015).

[25] Higgins, S. 2015. Bitcoin Mining Pools Targeted in Wave of DDOS Attacks. http://www.coindesk.com/bitcoin-mining-pools-ddos-attacks/ (consultado 3 abril 2015).

[26] Chomczyk, A. 2013. Situación legal de bitcoin en Argentina. http://elbitcoin.org/situacion-legal-de-bitcoin-en-argentina/(consultado 3 abril 2015).

[27] BCRA. Monedas virtuales: Comunicación al público en general. www.bcra.gov.ar/bilmon/bm023000.asp (consultado 3 abril 2015).

[28] Glickhouse, R. 2013. Explainer: Broadband Internet Access in Latin America. http://www.as-coa.org/articles/explainer-broadband-internet-access-latin-america (consultado 3 abril 2015).

[29] Palmer, D. Economist Nouriel Roubini Slams Bitcoin, Calls it a 'Ponzi Game' http://www.coindesk.com/economist-nouriel-roubini-slams-bitcoin-calls-ponzi-game/(consultado 3 abril 2015).

[30] Chavez-Dreyfuss, G. 2015. Exclusive: IBM looking at adopting bitcoin technology for major currencies. http://mobile.reuters.com/article/idUSKBN0M82KB20150312?irpc=932 (consultado 13 marzo 2015).

Bibliografía General

Bitcoin Organización.https://bitcoin.org/es/ (consultado 15 agosto 2014).

Bitcoin Foundation. https://bitcoinfoundation.org/ (consultado 15 agosto 2014).

Bitcoin News https://bitcoins.am/ (consultado 13 marzo 2015).

Bitcoin Wiki. https://en.bitcoin.it/wiki/Main_Page (consultado 25 agosto 2014).

Cointelegraph. http://cointelegraph.com (consultado 3 abril 2015).

CVE Detail. http://www.cvedetails.com/ (consultado 3 abril 2015).

ONG Bitcoin Argentina. http://www.bitcoinargentina.org/ (consultado 11 agosto 2014).

Litecoin. https://litecoin.org/ (consultado 15 febrero 2015).

Namecoin. https://namecoin.info/ (consultado 25 febrero 2015).

Peercoin. http://peercoin.net/ (consultado 15 febrero 2015).

SafeCurves: http://safecurves.cr.yp.to/rigid.html / (consultado 25 abril 2015).

Tail. https://tails.boum.org/ (consultado 21 febrero 2015).

Techtarget. Malware glossary. http://whatis.techtarget.com/glossary/Malware

TOR. https://www.torproject.org/ (consultado 15 febrero 2015).