DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN: ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

TEMA: DISEÑO DE UN POOL DESENTRALIZADO PARA CRIPTOMONEDAS, QUE UTILICE UN ALGORITMO DE SALTOS ENTRE POOLS

AUTOR: GARCÍA CHÁVEZ JUAN JOSÉ

TUTOR: DR. ESPINOSA O. NIKOLAI

SANGOLQUÍ-ECUADOR

2017

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

Certifico que el presente trabajo de investigación **DISEÑO DE UN POOL DESCENTRALIZADO PARA CRIPTOMONEDAS QUE UTILICE UN ALGORITMO DE SALTOS ENTRE POOLS,** realizado por el señor **Juan José García Chávez,** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditar y autorizar al señor **Juan José García Chávez** para que lo sustente públicamente.

Sangolquí, 16 de enero del 2017.

DR. NIKOLAI ESPINOSA O.

TUTOR DEL PROYECTO DE INVESTIGACIÓN

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

Yo **Juan José García Chávez,** con cédula de identidad N° 172098484-6 declaro que este trabajo de investigación **DISEÑO DE UN POOL DESCENTRALIZADO PARA CRIPTOMONEDAS QUE UTILICE UN ALGORITMO DE SALTOS ENTRE POOLS** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 16 de enero del 2017.

JUAN JOSÉ GARCÍA CHÁVEZ

C.C. 172098484-6

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

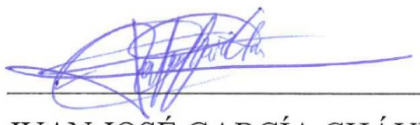
DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo **Juan José García Chávez,** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de investigación **DISEÑO DE UN POOL DESCENTRALIZADO PARA CRIPTOMONEDAS QUE UTILICE UN ALGORITMO DE SALTOS ENTRE POOLS** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 16 de enero del 2017.



JUAN JOSÉ GARCÍA CHÁVEZ

C.C. 172098484-6

DEDICATORIA

Este trabajo no hubiera sido posible sin el apoyo incondicional de mis Padres, por este motivo y al ser las personas que me han guiado desde mi nacimiento, quiero dedicarles completamente este trabajo de investigación y todo lo que se produzca a partir de él.

AGRADECIMIENTO

Primero a la Fuerza interior y universal que nos mantiene en constante movimiento, a mis Padres al que está dedicado este trabajo de investigación, a mi novia que me apoyo a pesar de mis locuras, a mi prestigiosa institución “Universidad de las Fuerzas Armadas ESPE”, porque en ella encontré una guía y los conocimientos que me permitieron llegar a este punto de mi investigación.

A todos mis docentes que compartieron sus conocimientos permitiéndome aclarar mis ideas y plasmarlas en este trabajo de investigación, para finalizar extiendo este agradecimiento para todas las personas que directa e indirectamente, me permitieron avanzar en este trabajo de investigación, el cual me ha dado mucha satisfacción personal y me llena de esperanza en lo que la humanidad y su tecnología es capaz de lograr.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

Este Trabajo de Investigación plantea el diseño de un pool de minería de criptomonedas descentralizado y que propone el uso de un algoritmo para el salto automático de pool de minería en redes P2P que utilizan el Protocolo Bitcoin. Para hacer ese salto, el algoritmo elige el mejor pool basándose en las estadísticas generadas durante su operación. Los experimentos para la validación y análisis de rendimiento del algoritmo se basan en redes de minería construidas específicamente para este fin. Los resultados principalmente indican que la generación de bitcoins alcanza hasta un 46% más que cuando se mina en un solo pool aislado. El diseño final propone, el uso del algoritmo para distintas criptomonedas y el manejo del pool a través de contratos inteligente.

Palabras Clave

- **BITCOIN**
- **HASH**
- **BLOQUE**
- **POOL DE MINERÍA**
- **SALTO DE POOLS**
- **CONTRATO INTELIGENTE**
- **APLICACIÓN DESCENTRALIZADA**

ABSTRACT

This research work proposes the design of a decentralized mining cryptocurrencies pool and proposes the use of an algorithm for automatic hopping among mining pools for P2P networks using the Bitcoin Protocol. To make that jump, the algorithm chooses the best pool based on the statistics generated during its operation. The experiments for validation and performance analysis of the algorithm are based on mining networks built specifically for this purpose. The results mainly indicate that the generation of bitcoins reaches up to 46% more than when it is mined in a single isolated pool. The final design proposes the use of the algorithm for different cryptocurrencies and the management of the pool through smart contracts.

Keywords

- **BITCOIN**
- **HASH**
- **BLOCK**
- **POOL OF MINING**
- **HOOP INTO POOLS**
- **SMART CONTRACT**
- **DESCENTRALIZED APPLICATION**

CAPÍTULO 1

INTRODUCCIÓN

1.1. ANTECEDENTES

Desde el surgimiento de herramientas como la Internet, la humanidad ha experimentado cambios fundamentales, uno de ellos es como los individuos interactúan unos con otros. Actualmente con la masificación de la Internet y las formas de pago digitales, las industrias relacionadas y tradicionales, han visto como el modelo de comercio tradicional va cediendo posiciones y está siendo cada vez más absorbido por esta nueva y más rápida forma de interacción de mercados.

El sistema financiero y económico también se ha ajustado a esta tendencia de globalización informática, la información de pagos, fundamental para que se realicen posibles intercambios de bienes y servicios, es transmitida en tiempos record, inimaginables en las décadas anteriores.

Lastimosamente el acceso y el manejo de estas herramientas, se ven limitadas a pocos emisores y no los suficientes usuarios. Los bancos y los emisores de tarjetas de crédito, se han esforzado por mejorar sus sistemas e infraestructuras de red, esto se da para acelerar la bancarización de sus clientes y captar más clientes, sin embargo este esfuerzo y junto a las regulaciones necesarias para prevenir delitos, no han permitido que la mayoría de posibles usuarios gocen de los beneficios de las plataformas de comercio electrónico con sistema financiero vigente.

Todo mencionado anteriormente, junto con la creciente seguridad necesaria para el correcto funcionamiento de las infraestructuras bancarias y junto a la cada vez mayor digitalización del dinero, han hecho que los medios tradicionales de pago den paso a innovaciones como: las tarjetas de crédito, e-banking, PayPal, etc.

La red que usa la criptomoneda bitcoin es una red peer-to-peer (P2P) y permite realizar transacciones financieras basadas bitcoins. Esta red es manejada siguiendo los lineamientos de un protocolo que recibe el mismo nombre, Protocolo Bitcoin. El

proceso de generación de las criptomonedas se denomina Minería. Un minero se refiere al equipo computacional que se utiliza para realizar la Minería. Un Pool de minería es una agrupación de mineros que juntan sus capacidades computacionales para hacer esta actividad más eficiente y rentable.

Matemáticamente, el proceso de minería implica solucionar el problema criptográfico denominado Prueba de Trabajo, este consiste en encontrar un producto de una función criptográfica llamado Hash, el algoritmo usado por el protocolo Bitcoin se llama SHA(256), que está conformado por 256 bits y el Hash buscado tiene cierta cantidad de ceros a su inicio, la cantidad de ceros está definida por la Dificultad del problema llamado Prueba de Trabajo. Para encontrar dicho producto, se valida un conjunto de transacciones que se conoce como Bloque. Una vez generado el bloque se lo agrega a la llamada cadena de bloques en ingles Blockchain, la cual tiene todo el historial de las transacciones realizadas y los bloques generados desde el lanzamiento e implementación del Protocolo Bitcoin en 2009.

La Dificultad de la Prueba de Trabajo causó que los equipos necesarios para minar ya no sean suficientes para que esta actividad sea rentable, es cuando se diseñaron los Pools de minería. Al usar un solo pool, la capacidad de generación de criptomonedas se ve limitada por los mineros que conforman el pool en cuestión. Con el desarrollo del algoritmo de salto entre pools se alcanzó hasta un 46% de rendimiento superior a cuando se mina en un solo pool aislado.

En una segunda etapa de la investigación, la evolución de las criptomonedas para crear aplicaciones distribuidas, es la base del desarrollo de un pool que permita minar no solo bitcoin sino cualquier criptomoneda y además sea capaz de descentralizar la actividad de minado, actualmente concentrada en grandes centros de datos.

En la etapa final del diseño se describen los elementos, que pueden hacer posibles la implementación de un pool descentralizado, el estudio de diferentes tipos de contratos inteligentes junto con los aspectos técnicos que lo hacen viable.

1.2. PLANTEAMIENTO DEL PROBLEMADE INVESTIGACIÓN

En la actualidad la minería de criptomonedas es una actividad muy especializada y con pocos participantes esto dista de la idea original expuesta en "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008) por Satoshi Nakamoto. La centralización de la minería requiere soluciones técnicas y de infraestructura de la red, lo más importante es agregar participantes al sistema para además de ampliar más la red P2P, agregar confiabilidad y robustez a la plataforma, logrando así una o varias plataformas descentralizadas que desconcentren la actividad de minería.

1.3. JUSTIFICACIÓN

Actualmente el ecosistema de las criptomonedas está definido por sus usuarios y sus usos. Internacionalmente su uso está regulado por muchos países, esto ha permitido a vista de los más entendidos un florecimiento de un nuevo tipo de economía.

Técnicamente bitcoin y el resto de criptomonedas existentes aun enfrentan grandes desafíos técnicos, de seguridad y adopción. Sin embargo al ser bitcoin y el protocolo Bitcoin de código abierto, su desarrollo ha permitido innovar alrededor del mundo a una velocidad nunca antes vista en productos financieros, que tradicionalmente han funcionado tanto sobre internet como en intranets.

Uno de los mayores problemas que enfrenta bitcoin son la escalabilidad y seguridad, respecto a ataques hipotéticos. Esta investigación se centra en la minería de criptomonedas en general y como descentralizar, optimizar y extender esta actividad.

1.4. ALCANCE

El desarrollo de un algoritmo que permita el salto entre pools de minería de bitcoin es el primer paso para el diseño de un pool descentralizado, si este sigue los lineamientos de P2Pool, que es el primer pool descentralizado para minería de bitcoin, además si se integra a las criptomonedas más populares y siempre permitiendo el acceso a la plataforma a nuevas criptomonedas, con la introducción de contratos inteligentes.

Se analizarán algunas alternativas para integrar los elementos necesarios de la plataforma, con algo fundamental para su funcionamiento que son los contratos inteligentes, estos fueron introducidos por la plataforma Ethereum desde el año 2013 (Wood, Ethereum: A secure decentralised generalised transaction ledger, 2015). Existen alternativas como Rootstock Plataform (Lerner, 2015), que mantienen la idea de los contratos inteligentes usando la blockchain más estable que existe hasta la actualidad y es decir la blockchain de bitcoin.

En el diseño de la plataforma que integre las herramientas analizadas en este trabajo de investigación se mencionaran al finalizar este trabajo de investigación.

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Diseñar una plataforma descentralizada que integre las tecnologías de criptomonedas, contratos inteligentes y redes p2p, con el uso de un algoritmo de salto entre pools.

1.5.2. OBJETIVOS ESPECÍFICOS

- Describir cómo funcionan los sistemas distribuidos, mostrando sus aplicaciones prácticas y usos actuales, además los elementos del Protocolo Bitcoin, para entender su potencialidad como sistema descentralizado.
- Indagar en el funcionamiento de los pools de minería de criptomonedas, conociendo su estructura y modelo de funcionamiento.
- Diseñar y probar un algoritmo que permita optimizar la minería de criptomonedas.
- Establecer los lineamientos necesarios para que pueda funcionar una plataforma descentralizada y además pueda implementar el algoritmo diseñado en la primera etapa.
- Integrar todos los elementos necesarios para el diseño de un pool descentralizado para criptomonedas y además use el algoritmo implementado en la primera etapa de la investigación.

CAPÍTULO 2

MARCO TEÓRICO

2.1. MODELO OSI Y FUNCIONAMIENTO DE INTERNET

El modelo OSI (Open Sistem Interconnection) es el modelo estructural teórico, para los protocolos de toda red de arquitectura.

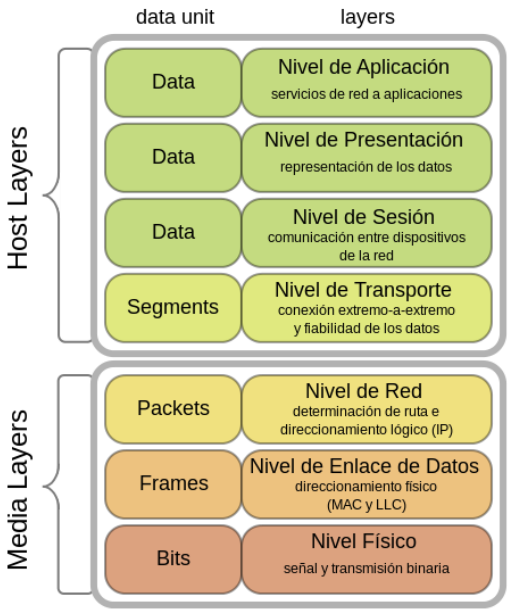


Figura 1 Modelo OSI
Fuente: (Stevens, 2012)

La Internet, que creció de la mano con el avance de las tecnologías de comunicación de Datos. A nivel usuario, la capa de Aplicación es con la que más es con la que más se interactúa y en la que se desarrollaron las aplicaciones descentralizadas. El funcionamiento de Internet actualmente se ha dado gracias a la implementación del modelo TCP/IP.

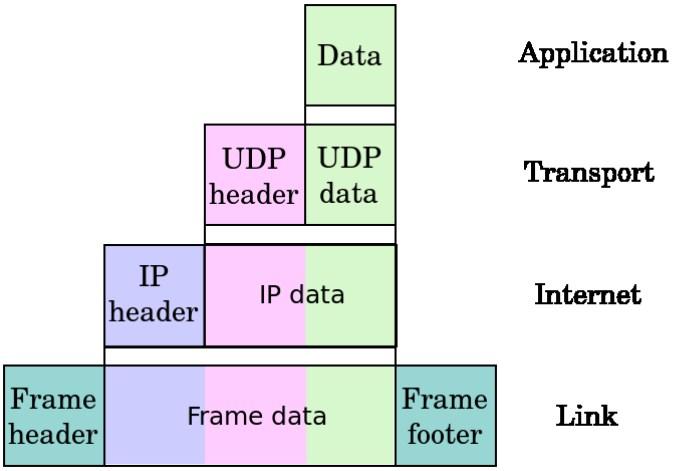


Figura 2 Modelo TCP/IP
Fuente: (Stevens, 2012)

Tradicionalmente las aplicaciones que funcionan sobre la Internet usan el modelo cliente-servidor para su funcionamiento, es aquí cuando los prestadores de servicios web han ampliado sus infraestructuras de red y además extendieron sus centros de datos a niveles nunca antes vistos.

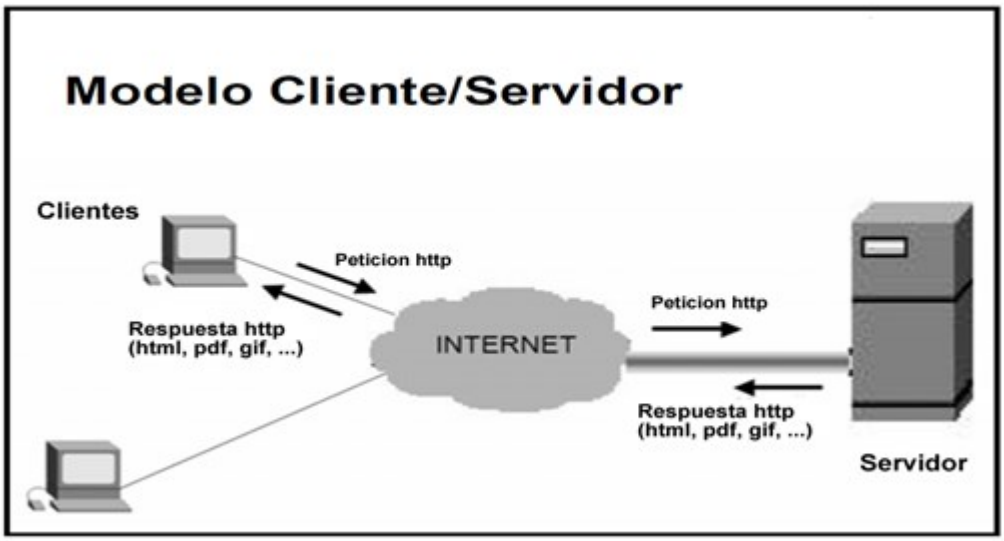


Figura 3 Modelo Cliente/Servidor
Fuente: (Stevens, 2012)

El área de tecnologías de la información se ha acelerado mucho, desde el surgimiento de internet como el medio masivo, que más interactúa con los usuarios. Los servicios

que se ofrecen en línea son diversos y las transacciones que se producen en la red son un punto crítico de la industria.

La manera en que se implementaron las aplicaciones que funcionan sobre una red, dio lugar a varios modelos de aplicación. Específicamente los P2P tuvieron un auge con la transferencia y compartición de archivos.

El modelo cliente-servidor se convirtió en la tónica de los servicios web, sin embargo las aplicaciones par a par (P2P) permiten que los usuarios no dependan de un servidor para correr la aplicación que se necesite.

Los modelos de funcionamiento de aplicaciones sobre cualquier red han evolucionado a tal punto que en la actualidad se manejan en mayoria los tres modelos que se obserban en la Figura 4.

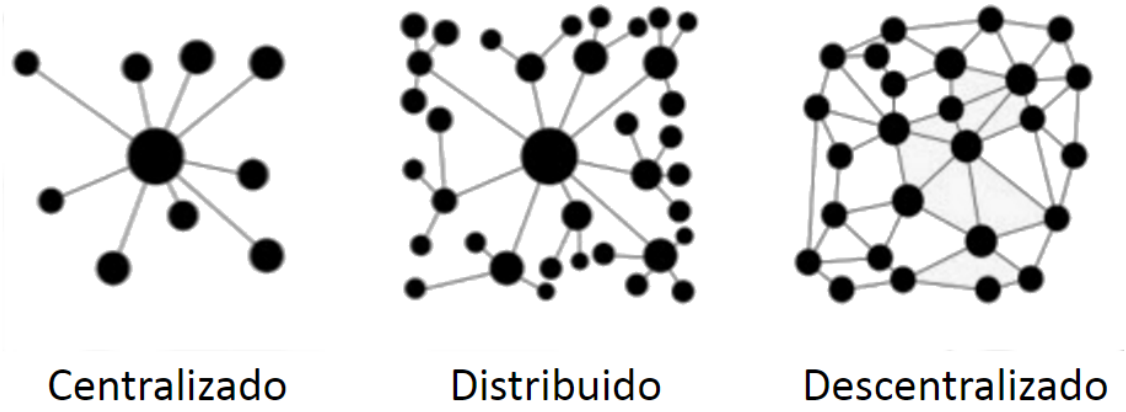


Figura 4 Modelos de red
Fuente: (Stevens, 2012)

Los servicios Web masivos dieron lugar a las aplicaciones distribuidas, este modelo de servicio mantiene hasta cierto punto el modelo cliente-servidor y una sola organización o empresa maneja y administra el sistema distribuido.

Un modelo descentralizado completamente es aquel que su manejo y administración no depende completamente de una organización, sino que todos los usuarios del sistema puedan llegar a un consenso para su correcto funcionamiento el Protocolo Bitcoin establece soluciones para llegar al consenso necesario en una aplicación transaccional.

2.2. CRIPTOGRAFIA Y SUS APLICACIONES ACTUALES

La Criptografía, literalmente significa “escritura oculta”, es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura de forma tal que solo puedan ser leídos por las personas a quienes van dirigidos.

La criptografía comprende dos sistemas:

- Sistema de cifrado simétrico: También llamado sistema de clave privada, Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Tanto el emisor como el receptor se comunican para ponerse de acuerdo sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave. Este sistema garantiza Confidencialidad e Integridad.

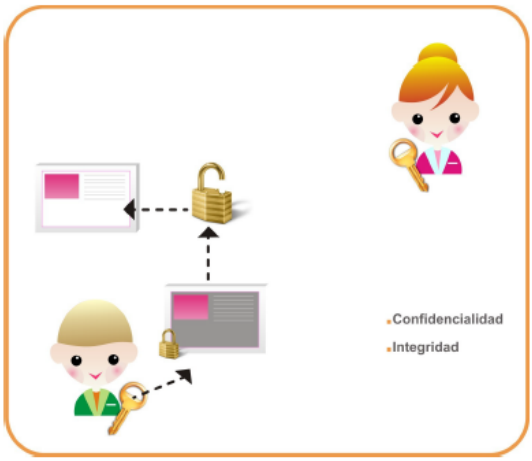


Figura 5 Criptografía Simétrica
Fuente: (Page, The International PGP Home, 2016)

- Sistema de cifrado asimétrico: También llamado sistema de clave pública, usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y la conoce cualquier destinatario, la otra clave es privada, solo la posee el emisor, debe guardarla con alto grado de seguridad de modo que ningún intruso tenga acceso

a ella. Los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje e integridad.

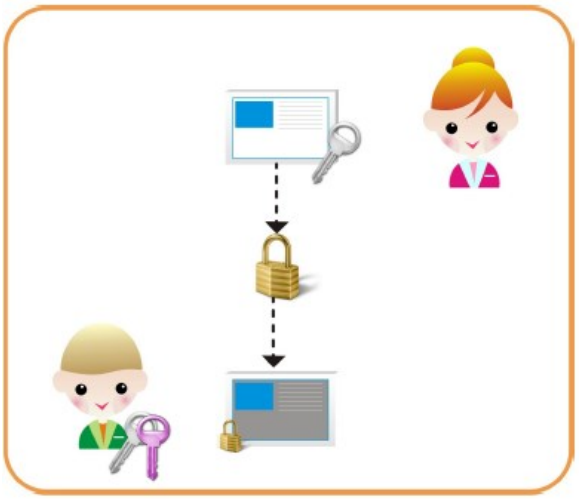


Figura 6 Criptografía Asimétrica
Fuente: (Page, The International PGP Home, 2016)

2.2.1. FIRMA DIGITAL

Una firma digital certifica un documento y lo atribuye fehacientemente a su autor. Con la firma digital se puede atribuir el documento a su autor de manera fehaciente, verificar que el contenido del documento no fue alterado y garantizar que el autor no pueda negar haber firmado el documento o mensaje.

Para esto se utiliza funciones de hash, que toman una entrada y retornan un string de longitud fija, conocida como “message digest”. Es fácil de calcular y es imposible de obtener el mensaje original a partir del hash. (Page, The International PGP Home, 2016) Los más utilizados actualmente son SHA-256, SHA-512.

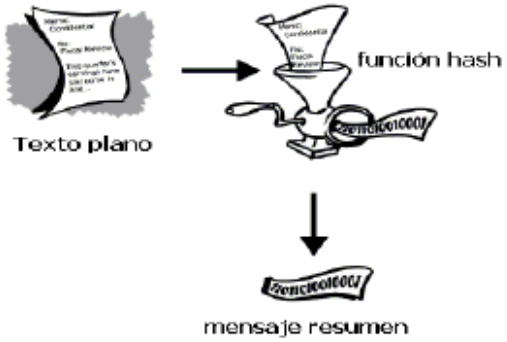


Figura 7 Función Hash
Fuente: (Page, The International PGP Home, 2016)

Proceso de firmar digitalmente: Se necesita que el emisor tenga un par de firmas (pública y privada). Se crea un hash del mensaje original, el emisor encripta el resumen del mensaje con su clave privada, y se envían al receptor.

Estos son llevados a cabo automáticamente por los módulos del hardware y/o software intervinientes.

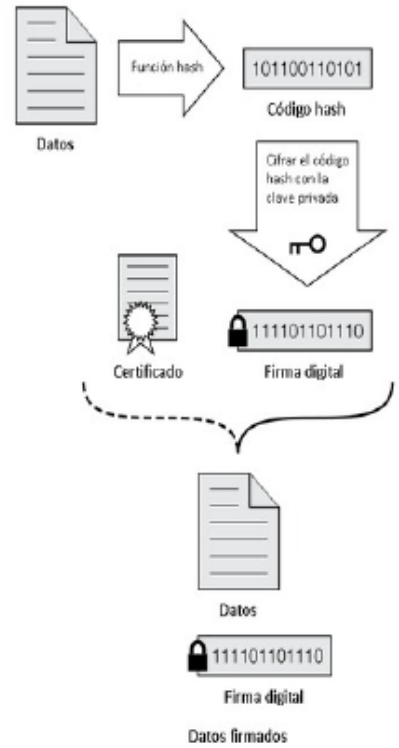


Figura 8 Proceso de Firma Digital
Fuente: (Page, The International PGP Home, 2016)

Por otra parte el receptor utiliza la clave pública del emisor para descencriptar la firma digital, y el sistema calcula un nuevo resumen a partir del mensaje recibido y verifica que coincida con el hash que recibió y si coincide significa que la firma es válida y el mensaje no fue alterado.

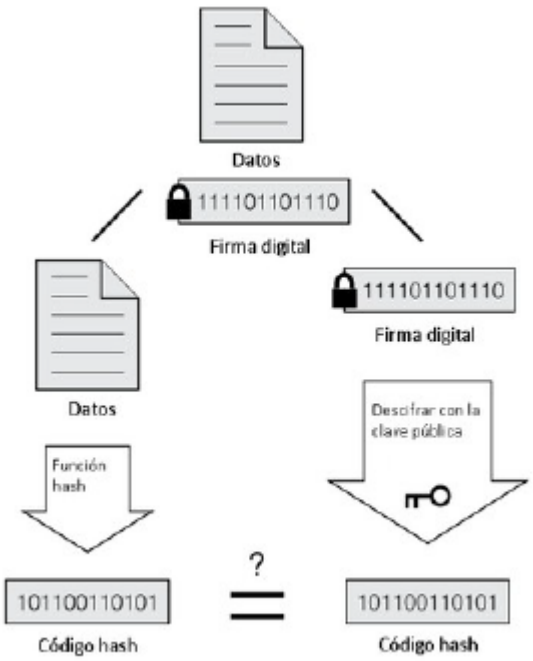


Figura 9 Comprobación de Firma Digital

Fuente: (Page, The International PGP Home, 2016)

2.3. PROTOCOLO BITCOIN Y FUNCIONAMIENTO DE CRIPTOMONEDAS

El bitcoin es la primera moneda digital basada en el uso de la criptografía. De hecho, bitcoin es la primera implementación de una criptomoneda, esta usa los lineamientos del Protocolo Bitcoin para su funcionamiento. A diferencia de la mayoría de las monedas convencionales bitcoin está diseñada para trabajar sobre una red P2P. Es decir, bitcoin no está controlada por una autoridad central, que regule la emisión de moneda. Ni pone restricciones en las transacciones que sobre ella se realizan, a diferencia de los bancos privados y emisores de tarjetas de crédito. La red sobre la que funciona bitcoin permite observar todas las transacciones que se llevan a cabo, gracias a su cadena de bloques o más conocida como blockchain, esta es pública y además blockchain mantiene la privacidad y anonimato de sus usuarios.

El articulo original donde se plasman los elementos necesarios para la implementación de la criptomoneda bitcoin "Bitcoin: A Peer-to-Peer Electronic Cash System", tiene como elementos fundamentales los siguientes:

- Transacciones.
- Estampa de tiempo (Timestamp server).
- Prueba de Trabajo (Proof of Work).
- Cadena de Bloques (blockchain)
- Funcionamiento de la red P2P.
- Incentivo.

Los elementos mencionados ya permiten el funcionamiento de bitcoin sin embargo el desarrollo del protocolo Bitcoin requirió de muchos más lineamientos que se encuentran documentados en sus BIPs(Bitcoin Improvement Proposals), estos han sido lo que han producido el éxito de su implementación.

El equipo de desarrollo encargado de la implementación ha contado con desarrolladores y criptógrafos de gran nivel, este es un factor determinante en la llevada a cabo de un sistema transaccional descentralizado nunca antes visto.

2.3.1. DIRECCIONES

Las direcciones Bitcoin generadas correctamente proceden de un número secreto llamada clave privada, un tipo de clave criptográfica que se utiliza una firma electrónica, y que es la única información necesaria para poder gastar los fondos asociados a la dirección. Cuando se utiliza un programa cliente de Bitcoin, las claves privadas se guardan en un tipo de archivo llamado archivo monedero. El monedero consta de una clave pública y una clave privada. La clave privada es imprescindible para crear nuevas transacciones que envíen bitcoins de una dirección a otra. Si se pierde la clave privada correspondiente a una dirección (por ejemplo, por una avería o un accidente como un incendio o una inundación que destruya el dispositivo), los bitcoins en esa dirección se pierden para siempre, sin embargo existen métodos de almacenar los monederos offline conocidos como monederos en frio.

Una dirección de bitcoin es un identificador de entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3, que representa un destino u origen de un pago en bitcoins. Las direcciones se pueden generar muy fácilmente (prácticamente instantáneamente) y en número arbitrario desde cualquier programa cliente de bitcoin, a través de servicios en Internet o monederos en línea. Además es posible hacerlo offline. Las direcciones aparecen por primera vez en la red bitcoin cuando forman parte de una transacción, no generan gastos ni contienen información personal del usuario y son generalmente anónimas. Pueden usarse para un solo uso y luego ser desechadas y no volver a usarse nunca más y cuando no ha sido usada nunca no aparece en la red bitcoin.

El total de direcciones diferentes que pueden existir en la red bitcoin es 2^{160}. Una de las dudas iníciales que contemplé fue que si no hay ninguna entidad central que controla la creación de direcciones y esto se hace de manera individual, es decir, es posible que dos usuarios diferentes generen la misma dirección. Es improbable que se generen 2 direcciones iguales por la cantidad que existen y por el diseño de las mismas.

2.3.2. ALGORITMO DE CURVA ELIPTICA EN FIRMAS DIGITALES (ECDSA)

ECDSA es el algoritmo criptográfico usado por Bitcoin para asegurar que solo puede gastar los fondos el dueño legítimo de estos. En ECDSA encontramos los siguientes conceptos clave: Clave privada: Es un número secreto, que sólo conoce la persona que lo ha generado. Una clave privada es esencialmente un número generado aleatoriamente o elegido por el usuario que lo genera. Es posible generar clave privadas escribiendo un texto que podemos recordar. En bitcoin solo la persona con la clave privada que está asociada a unos fondos podrá gastarlos. En bitcoin, una clave privada es un entero de 256 bits (32 bytes).

Clave pública: Es un número que está asociado a una clave privada, pero que puede ser anunciado y compartido. Una clave pública se puede calcular a partir de una clave privada, pero no viceversa. Una clave pública se puede utilizar para determinar si una firma es auténtica (en otras palabras si se ha generado usando la clave privada concreta) sin requerir la clave privada para ser comprobado. En bitcoin, la clave pública se puede representar de manera comprimida o sin comprimir. Las claves públicas comprimidas son de 33 bytes, que consta de un prefijo o bien 0x02 o 0x03, y un entero de 256 bits llamado x. Las claves sin comprimir son de 65 bytes, que consta de prefijo constante (0x04), seguidas de dos números enteros de 256 bits llamados “x” e “y” (2 * 32 bytes). El prefijo de una clave comprimido permite calcular el valor de “y” a partir del valor “x”.

Firma: Es un número que demuestra que un mensaje ha sido creado por un usuario concreto. Una firma es generada matemáticamente a partir de un hash de algo que debe ser firmado y de la clave privada. La firma en si, consiste en dos números conocidos como “r” y “s”. Usando la clave pública y un algoritmo matemático se puede verificar que dicha firma ha sido realizada con la clave privada y con el hash de lo que se pretendía firmar. Las firmas son de 73, 72, o 71 bytes de longitud, con probabilidades aproximadamente el 25%, 50% y 25%, respectivamente, aunque tamaños aún más pequeños son posibles con probabilidad decreciente exponencialmente.

Tabla 1
Elementos de Firma Digital en bitcoin.

Elemento	Función
Clave privada	Genera la clave pública Genera firmas (permite transferir dinero) No se puede compartir Si se pierde o destruye no se podrán recuperar los fondos
Clave pública	Identifica una clave privada Se usa para verificar firmas
Dirección	Es el identificador público del monedero Identificar la cuenta para enviar BTC
Firma	Permite verificar que un mensaje ha sido firmado por el propietario de la clave privada sin conocerla.

2.3.3. DIRECCIÓN MULTIFIRMA

Se pueden generar direcciones que requieran una combinación de varias claves privadas. Este tipo de direcciones dependen de algunas características añadidas al protocolo con posterioridad al lanzamiento original de bitcoin, por lo que se las diferencia de las direcciones originales a través de un carácter inicial '3', en lugar del '1' de las direcciones convencionales. Este tipo de direcciones avanzadas equivaldrían a un cheque con más de un beneficiario, para cobrar el cual hace falta la firma de todos los beneficiarios. El requisito concreto, como el número de claves privadas necesario para acceder a los fondos, se decide al generar la dirección. Una vez creada, no es posible cambiar esos requisitos de acceso a los fondos.

2.3.4. CODIFICACIÓN DE UNA DIRECCIÓN BITCOIN

Sería posible usar solo la clave pública para transferir dinero, pero en el protocolo bitcoin se creó las direcciones. Ello es por una razón concreta. Las direcciones bitcoin tienen una codificación especial. Bitcoin usa la codificación de binario a texto Base58. La respuesta de porque no se usa la base-64 la encontramos en el código fuente del cliente de bitcoin.

Las principales razones son:

Se eliminan los caracteres que se parecen para evitar el error humano al copiarlas.

Se parecen a números de cuenta a los que las personas están más acostumbrados al no usar símbolos especiales y ser solo alfanumérico.

En la Figura 10 se puede observar cuales son las funciones matemáticas para obtener la dirección de un monedero a partir de su clave pública.

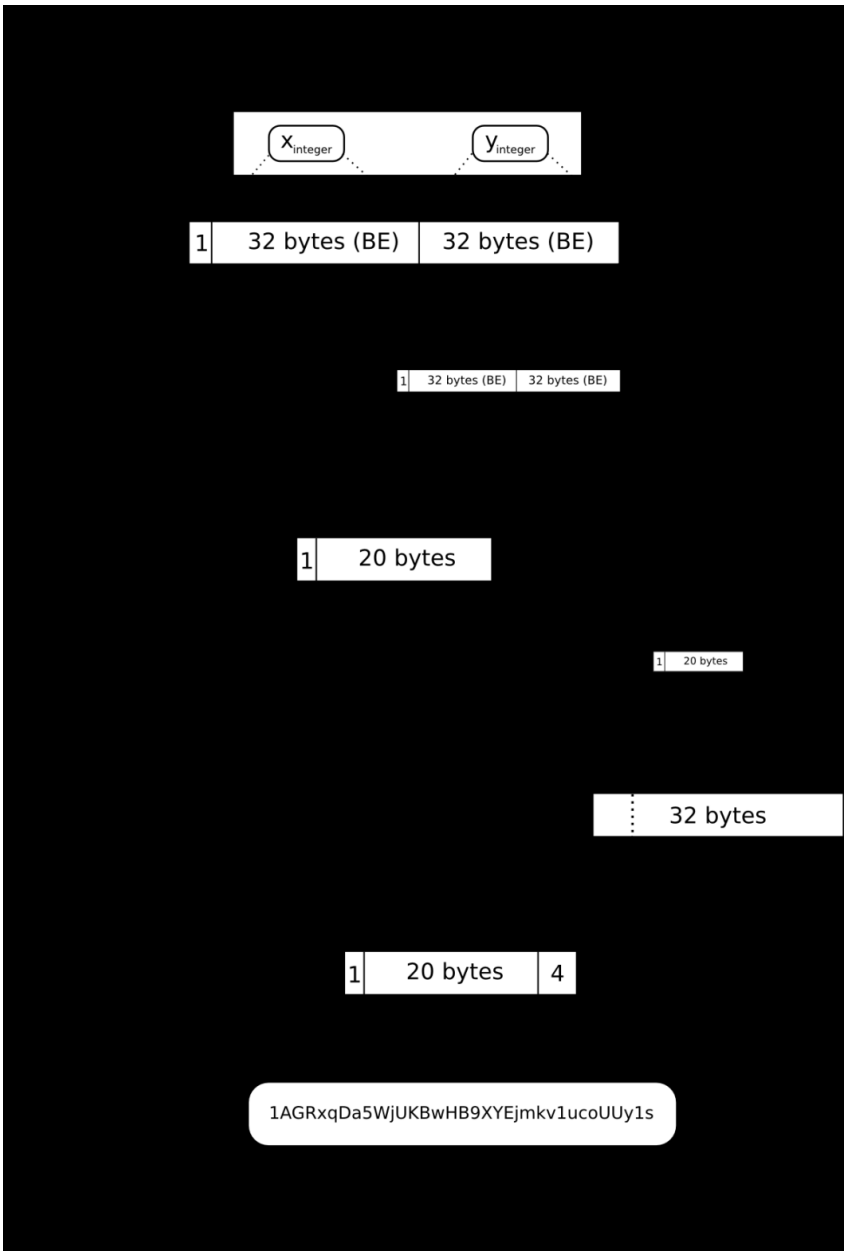


Figura 10 Llave pública a dirección de monedero

Fuente: (Antonopoulos, 2014)

2.3.5. TRANSACCIONES

Las transacciones realizadas por los usuarios de bitcoin son difundidas por los nodos donde se generan hacia todos los demás nodos que conforman la red P2P, para que una transacción sea dada como válida debe ser incluida en un bloque y verificada por todos o al menos la mayoría de nodos mineros, este es el consenso al que se debe llegar utilizando mecanismos expuestos más adelante.

Las transacciones son líneas en un libro contable de doble entrada. Es decir, cada transacción contiene una o más entradas (inputs), que son débitos contra un monedero bitcoin. En el otro lado de la transacción, hay una o más salidas (outputs), que son créditos añadidos al otro monedero bitcoin. Las entradas y salidas (débitos y créditos) no suman necesariamente la misma cantidad y su diferencia es entregada a los mineros como una comisión de transacción implícita, esta diferencia es tomada por el minero que incluye la transacción en la blockchain, al encontrar un bloque.

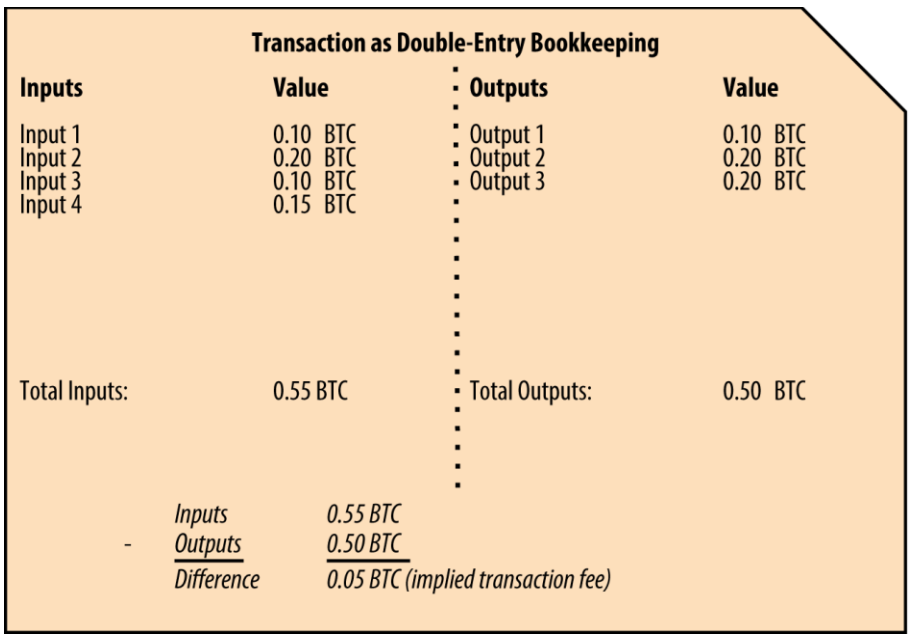


Figura 11 Ejemplo de transacción de doble entrada.

Fuente: (Antonopoulos, 2014)

En la Figura 11 se observa claramente cómo se manejan las transacciones en el Protocolo Bitcoin además las transacciones se encuentran enlazadas unas a otras por las firmas y verificaciones de la manera que se indica en la Figura 12 .

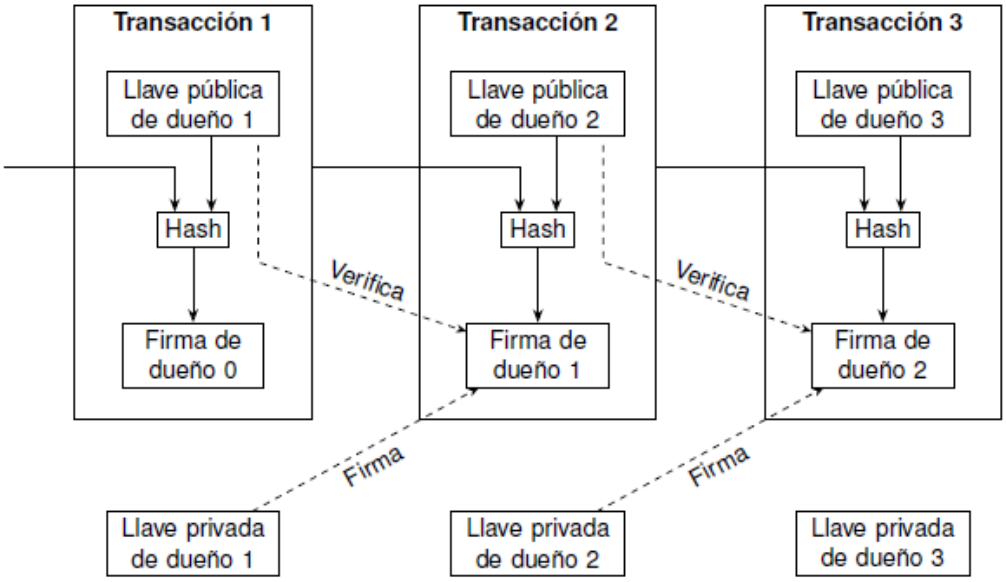


Figura 12 Transacciones encadenadas
Fuente: (Nakamoto, 2008)

Gracias a las llaves públicas y privadas cada transacción tiene un sentido de pertenencia único e irrepetible esto se da por las técnicas criptográficas usadas por el protocolo Bitcoin, el trabajo que realizan los mineros es verificar que las firmas de las transacciones sean válidas y producidas por la llave publica del usuario que está realizando la transacción.

2.3.6. ALGORITMO DE PRUEBA DE TRABAJO

Cuando se producen las transacciones como se explicó en la sección anterior las transacciones no son agregadas a la cadena de bloques hasta que un minero resuelva la denominada Prueba de Trabajo, el sistema de confianza de bitcoin se basa en la capacidad informática. Las transacciones son empaquetadas en bloques, que requieren una enorme capacidad de computacional para ser encontrados, pero solo con una

pequeña capacidad computacional se los puede validar. El proceso de minería tiene dos propósitos en bitcoin:

- La minería crea nuevos bitcoins en cada bloque, es la manera como se obtiene ganancias minando, es decir es el incentivo para el minero. La cantidad de bitcoin creados por bloque es fijo y disminuye con el tiempo.
- La minería crea confianza asegurando que las transacciones se confirman al dedicar el suficiente poder computacional al bloque que lo contiene.

El minero construye un bloque candidato lleno de transacciones. A continuación, el minero calcula el hash de la cabecera de este bloque y ve si es más pequeño que el objetivo actual. Si el hash no es menor que el objetivo, el minero modificará el nonce (por lo general incrementando solo por uno) y lo intentará de nuevo. Para la dificultad actual en la red bitcoin, los mineros tienen que intentar trillones de veces antes de encontrar un nonce que produzca un hash de cabecera de bloque lo suficientemente bajo. El nonce es un el valor que se va modificando para hallar el hash esperado y definido por la dificultad que a su vez por diseño está programada para que cambie de valor cada 2016 bloques además de mantener en promedio la generación de un bloque cada 10 minutos (A.Back, 2012).

2.3.7. CADENA DE BLOQUES

La cadena de bloques es uno de los elementos estructurales del protocolo bitcoin en ella se guardan todas las transacciones que se han producido en bitcoin o en cualquier otra implementación de criptomoneda. Gracias a la Prueba de trabajo se validan los bloques y se asegura el funcionamiento de la criptomoneda en la Figura 13 se tiene la estructura que se forma al encadenar los bloques de transacciones.

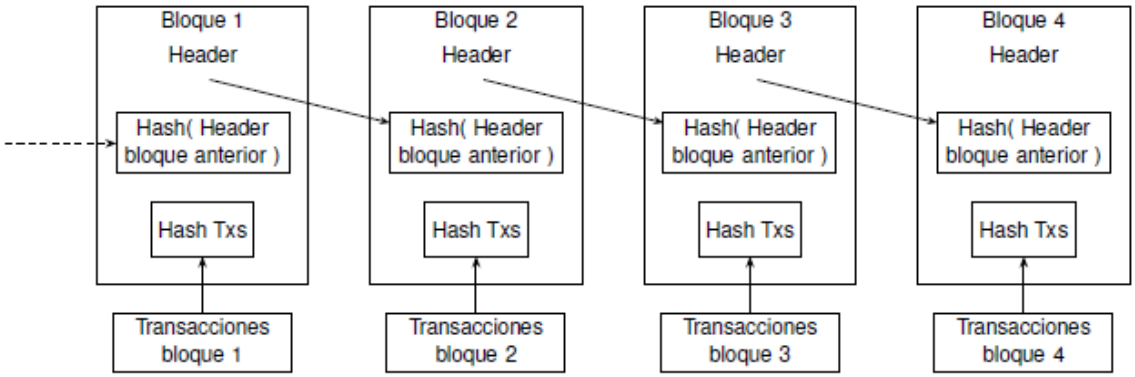


Figura 13 Cadena de bloques
Fuente: (Nakamoto, 2008)

2.4. MINERIA DE CRIPTOMONEDAS EN LA ACTUALIDAD

En la actualidad la actividad de generar bitcoin con equipos computacionales se ha desarrollado a tal nivel que las inversiones necesarias para incursionar en minería llegan a un valor de varios millones de dólares.

El algoritmo Prueba de Trabajo (PoW) es determinante en la minería de bitcoin este consiste en resolver un problema criptográfico que además representa una solución a la computación distribuida como se menciona en Mastering Bitcoin (Antonopoulos, 2014):

Una Solución a un Problema de Computación Distribuida

> La invención de Satoshi Nakamoto es también una solución a un problema previamente sin solución en computación distribuida, conocido como el "Problema de los Generales Bizantinos." Brevemente, el problema consiste en tratar de llegar a un consenso al respecto de un plan de acción intercambiando información a través de una red poco fiable y potencialmente comprometida. La solución de Satoshi Nakamoto, que utiliza el concepto de prueba de trabajo para alcanzar un consenso sin requerir confianza en una autoridad central, representa un avance en computación distribuida y posee amplias aplicaciones más allá de las monedas. Puede ser utilizada para alcanzar consenso en redes distribuidas para probar la legitimidad de elecciones, loterías, registros de activos, autorizaciones bajo notario digitales, y más. (p4)

Aunque los nodos en la red P2P bitcoin son iguales, puede que asuman roles distintos dependiendo de la funcionalidad que soporten. Un nodo bitcoin es una colección de funciones: enrutamiento, la base de datos de la cadena de bloques (en inglés, "blockchain"), minado y servicios de cartera.

Un nodo completo con todas estas funciones se detalla en Un nodo de la red bitcoin con todas sus cuatro funciones: monedero, minero, base de datos de cadena de bloques completa, y enrutamiento de red.

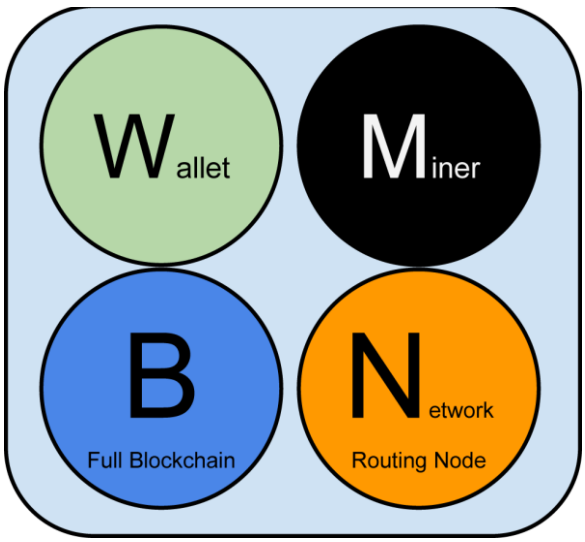


Figura 14 Nodo con las 4 funciones posibles de un nodo
Fuente: (Antonopoulos, 2014)

Los usuarios con más experiencia usan cualquier combinación posible de los 4 tipos nodos mostrados en la Figura 14, estos funcionan sobre la red bitcoin que se encuentra extendida alrededor del mundo y cuenta con alrededor de 7000 nodos funcionales.

Los nodos de Minería de color negro en la Figura 14 compiten para crear nuevos bloques ejecutando hardware especializado para resolver el algoritmo de prueba de trabajo. Algunos nodos de minería son también nodos completos es decir, mantienen una copia completa del blockchain y minan independientemente, mientras que otros son nodos ligeros que participan en un pool de minería y el pool es el que mantiene un nodo completo.

Con la expansión de los pools de minería la cantidad de nodos mineros ha decrecido, las empresas que ofrecen servicios con bitcoin se han convertido en las que respaldan el funcionamiento de la red, en la actualidad ya existen implementaciones de nodos ligeros que no necesitan tener la blockchain completa para funcionar.

En la minería con el desarrollo del Protocolo Stratum por parte de Slush Pool (Palatinus, 2010) ha permitido que no sea necesario un nodo completo para minar. A continuación se observara como se ha desarrollado la minería en sus diferentes etapas.

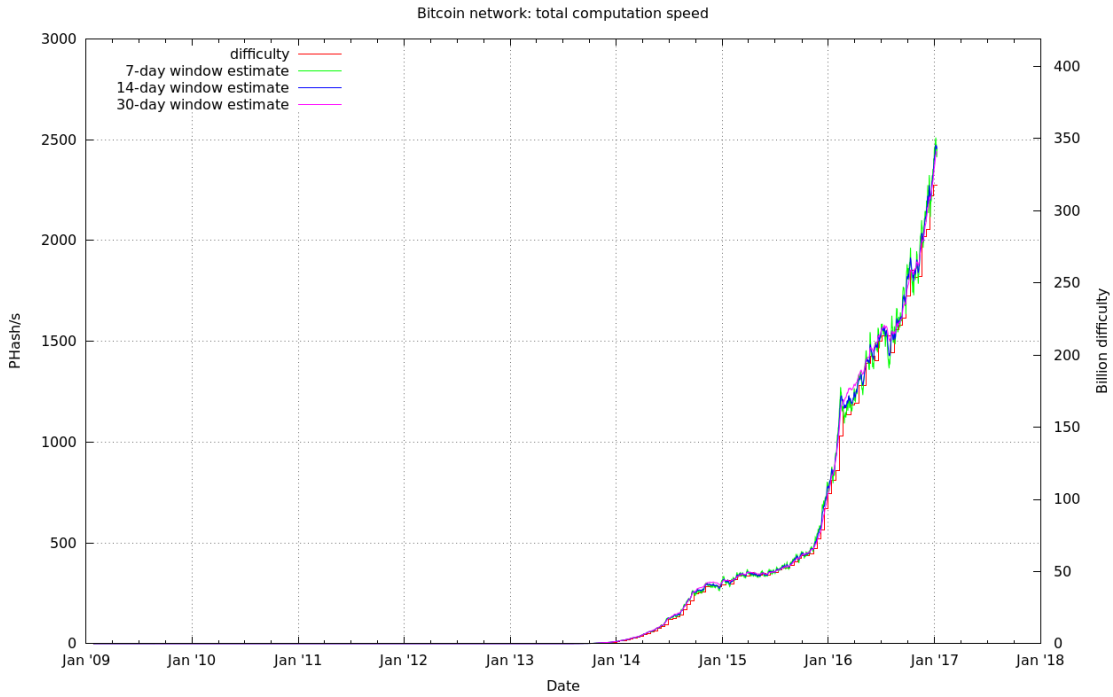


Figura 15 Histórico de velocidad de red bitcoin en PHs
Fuente: (Bitcoin Network Graphs, 2016)

Como se observa en la Figura 15 desde Enero del 2014 se da un despunte en la velocidad existente en la red esto se da principalmente por el desarrollo de mineros ASICs más eficientes y de mayor capacidad. Para una mejor apreciación a continuación se tiene la velocidad en escala exponencial.

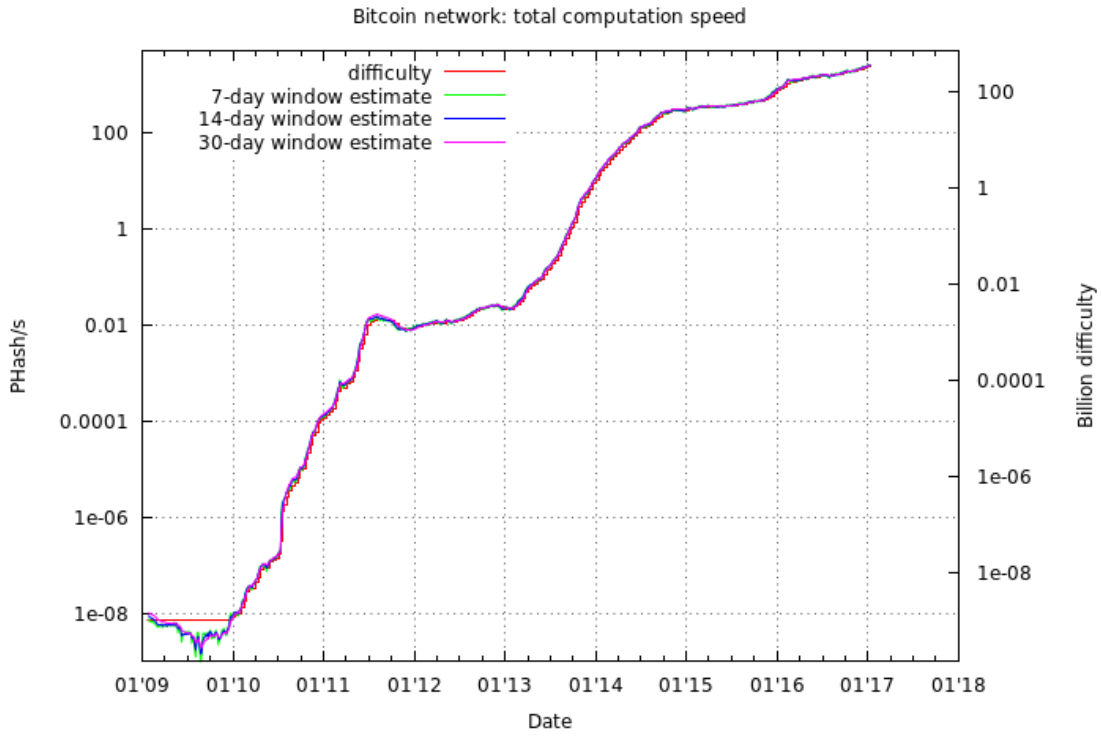


Figura 16 Velocidad en PHs en escala exponencial
Fuente: (Bitcoin Network Graphs, 2016)

Como se puede observar en la Figura 16 el eje vertical izquierdo muestra cual es el poder computacional de la red en orden de giga hashes por segundo. Se observa varias cosas las cuales han sido los momentos históricos de la red bitcoin. El Protocolo Bitcoin ajusta la dificultad para que en promedio se genere un bloque cada 10 minutos. La dificultad no vario durante aproximadamente los primeros 12 meses de vida hasta diciembre de 2009. En julio de 2010 por el creciente interés en bitcoin se ve como se dispara exponencialmente la capacidad computacional de la red.

Además durante el último semestre de 2010 un cliente GPU de minería fue lanzado permitiendo así el crecimiento de la capacidad de la red. El aumento de la dificultad en 2010, fue de 10.000 veces en un solo año, esto hace que surja el primer pool de minería (Palatinus, 2010) repartiendo así los bitcoins generados bloque entre los participantes. El 6 de marzo de 2011 en un periodo corto de tiempo la red alcanza un

record de 900Ghash/segundo para luego bajar a 500Ghash/ segundo. Se especula que alguna o varias supercomputadoras fueron conectadas a la red durante ese tiempo. Debido a esto la dificultad aumento por el diseño del protocolo Bitcoin y mantener estable el ratio de generación de bloques. Tras este periodo, se dio por primera vez un descenso en la dificultad en un 10%. A mediados de 2011 la dificultad se estabilizo alrededor de 1.000.000 y solo un año más tarde volvía a empezar a crecer de nuevo. Durante febrero de 2013 a Mayo de 2013 la dificultad se ha multiplicado por ~10. Este es debido a la inclusión de los nuevos equipos y técnicas de minado entre ellas FPGAs y la aparición de los primeros ASIC.

Figura 17 Chips ASIC marca Avalon para Minería.
Fuente: Avalon

Por ejemplo en julio de 2010 se detectó el primer bloque minado usando GPU y como vemos la dificultad creció de forma exponencial. El otro gran cambio ha sido la introducción de FPGA y ASIC, no obstante, este equipo solo están disponibles desde principios de 2013 y solo a ciertos usuarios. En la actualidad ya existen varias generaciones de equipos ASIC con un desarrollo nunca antes visto que supera en velocidad a la ley de Moore.

La dificultad de la red bitcoin se encuentra en un valor que alcanza los 350 Billones y la minería se ha convertido en una actividad especializada con grandes centros especializados ubicados en lugares donde la energía eléctrica es barata.

Figura 18 Ring de minería actual Suecia 2014
Fuente: Datavetaren.

2.5. APLICACIONES DESCENTRALIZADAS Y EL ROL DEL PROTOCOLO BITCOIN EN SU FUNCIONAMIENTO

Ethereum: Este sistema descentralizado se basa en un principio que es "El código es la ley", es decir lo que se plasma en el código informático de un contrato inteligente es lo que permite que una transacción se cumpla, no se cumpla o se cumpla parcialmente. Un contrato inteligente permite implementar aplicaciones descentralizadas que corran sobre la plataforma de Ethereum, esta es sostenida al igual que en bitcoin con el poder de computo de los mineros. (Ethereum community, 2016)

Ethereum es una plataforma Turing-completa de procesamiento y ejecución de contratos, basada en una cadena de bloques independiente a la existente en bitcoin. Ethereum tiene una criptomoneda incorporada, llamada ether, además de un mecanismo llamado GAS que es el combustible para la ejecución de contratos. La cadena de bloques de Ethereum registra los contratos, estos se expresan a nivel bajo, en un lenguaje Turing-completo, similar a un código de bytes. En esencia, un contrato es un programa que se ejecuta en cada nodo del sistema Ethereum. Los contratos Ethereum pueden almacenar datos, enviar y recibir pagos de ether, almacenar ether, y ejecutar una gama infinita (de ahi Turing-completo) de las acciones computables, actuando como agentes de software autónomos descentralizados.

Ethereum puede implementar sistemas bastante complejos que en otro caso se implementarían como cadenas alternativas. Por ejemplo, el siguiente caso es un contrato de registro de nombres similar a Namecoin escrito en Ethereum (o más exactamente, escrito en un lenguaje de alto nivel que puede ser compilado a código Ethereum).

Tabla 2
Ejemplo de contrato inteligente

```
if !contract.storage[msg.data[0]]: # .Ya está  tomada la clave?
    # ¡Entonces la tomamos!
    contract.storage[msg.data[0]] = msg.data[1]
    return(1)
else:
    return(0) // De lo contrario no hacer nada
```

Fuente: (Antonopoulos, 2014) p229

Rootstock: Es una implementación en fase de experimentación que implementa contratos inteligentes sobre la blockchain más estable que se conoce hasta la actualidad y esta es la blockchain de bitcoin, RSK es la primera plataforma de contratos inteligentes de código abierto con pegas de dos vías a bitcoin que también recompensa a los mineros de Bitcoin a través de la merge – mining que permite minar bitcoin en paralelo, esto permite participar activamente en la revolución de los contratos inteligentes. El objetivo de RSK es agregar valor y funcionalidad al ecosistema de Bitcoin al permitir contratos inteligentes, pagos casi instantáneos y mayor escalabilidad. (Lerner, 2015)

Tabla 3
Código en Derecho vs Código en Informática

	Código en Derecho	Código en informática
Lógica basada en	Mentes subjetivas, analogías	Lógica booleana, bits
Seguridad	Desacato / Prisión	Replicación + Criptografía
Predictibilidad	Flexible	Rígido
Madurez	Alta evolución / muchos casos	Primeras implementaciones / pocas experiencias
Área	Silos jurisdiccionales	Independencia de instituciones políticas y financieras, sin fronteras
Costos	Demandas: alto	Muy bajo

Fuente: (Nick Szabo, Devcon 1, Londres, Noviembre 2015)

2.6. POOL DESENTRALIZADO PARA BITCOIN (P2POOL)

Ante la creciente concentración de capacidad de procesamiento de los pools de minería, surgió la preocupación de un posible ataque hacia la red que soporta a bitcoin, este ataque es conocido como “ataque del 51%”, una de las cualidades del Protocolo bitcoin, es el consenso que debe existir con la generación de bloques, si un minero con la suficiente capacidad es decir al menos el 51% podría premeditadamente romper con el consenso y validar a su conveniencia los bloques que se producen. Un antecedente a esto fue cuando GHASH.io (pool de minería) estuvo a punto de llegar al 50% de la capacidad total de la red, GHASH.io pidió a sus usuarios cambiar de pool.

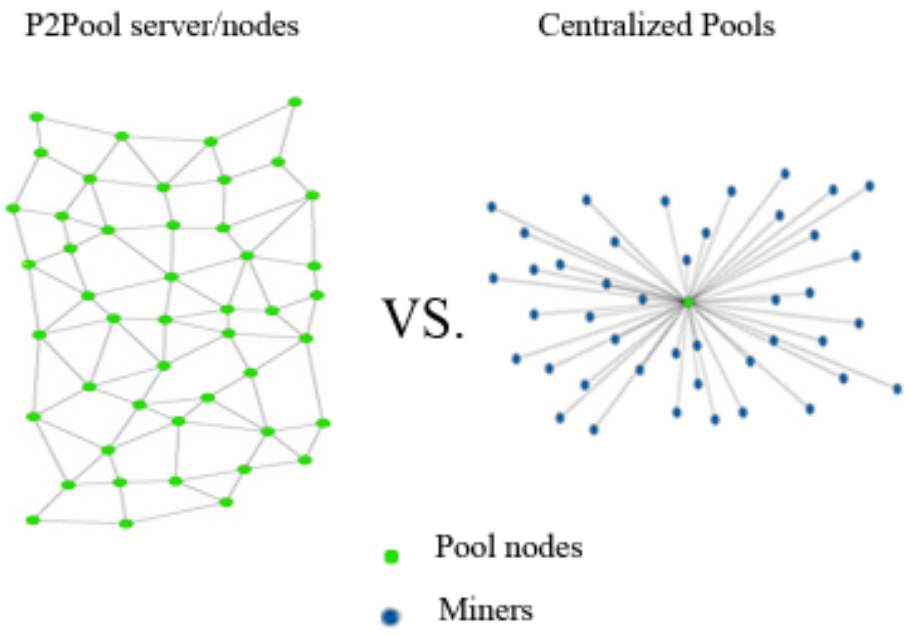


Figura 19 Modelo de Pool P2P versus Centralizado

Si el servidor del pool cae o se ralentiza por un ataque de denegación de servicio, los mineros del pool no pueden minar perdiendo así el trabajo realizado y por realizar. En 2011, para resolver estos problemas de la centralización, se propone y se implementa un nuevo método de minería de pool: P2Pool es un pool de minería de par a par, sin operador central.

P2Pool descentraliza las funciones del servidor de pool, implementando un sistema similar a una cadena de bloques paralela que se llama cadena de cuotas (en inglés, "share chain"). Una cadena de cuotas es una cadena de bloques que funciona a una dificultad más baja que la cadena de bloques de bitcoin.

La cadena de cuotas permite que los mineros del pool puedan colaborar en un pool descentralizado, minando cuotas en la cadena de cuotas a una velocidad de un bloque de cuota cada 30 segundos. Cada uno de los bloques en la cadena de cuotas registra una participación proporcional en la recompensa para los mineros del pool que contribuyen con trabajo, arrastrando las cuotas hacia adelante desde el bloque de cuota anterior. Cuando uno de los bloques de cuota alcanza también el objetivo de dificultad de la red bitcoin, se propaga y se incluye en la cadena de bloques de bitcoin, premiando a todos los mineros del pool que contribuyeron con todas las cuotas que precedieron al bloque de cuota ganador.

En vez de un servidor de pool que lleva el seguimiento de todas las cuotas y recompensas de los mineros del pool, la cadena de cuotas permite que todos los mineros del pool lleven el seguimiento de todas las cuotas utilizando un mecanismo de consenso descentralizado similar al mecanismo de consenso en la cadena de bloques de bitcoin. Este es uno de los mecanismos que se usara en el diseño del pool con la característica añadida del acceso a otros pools aprovechando así la capacidad existente en los demás pools.

CAPÍTULO 3

ALGORITMO DE SALTO AUTOMATICO ENTRE POOLS DE MINERIA DE BITCOIN

En esta, la primera etapa de la investigación se desarrolló y probo un algoritmo capas de elegir el mejor momento para cambiar de pool de minería de bitcoin, para esto se utiliza las estadísticas de generación de bitcoin. (García Chávez & Da Silva Rodrigues, A simple algorithm for automatic hopping among pools in Bitcoin mining network, 2015)

3.1. DESCRIPCION DEL ALGORITMO

Este Algoritmo que será descrito a continuación puede ser implementado en un ring de equipos de minería específicos para bitcoin, sin embargo podría ser usado para todo el ecosistema de criptomonedas existente en la actualidad. En el último capítulo de este trabajo de investigación se integra este algoritmo a una aplicación descentralizada.

A continuación se muestra sistemáticamente la forma de funcionamiento del algoritmo.

Tabla 4
Algoritmo de Salto automático de pools

Inicio
Paso 1: Capturar el tiempo que tardaron en generar los últimos bloques encontrados por los pools que van a ser considerados.
Paso 2: Calcular el Promedio y la Desviación Estándar del tiempo de generación de cada pool considerado con los datos obtenidos en Paso 1.
Paso 3: El pool cuyo tiempo de actual se acerque más al promedio y además tenga la desviación estándar más pequeña respecto a su promedio será el elegido para minar, en primera instancia.

Paso 4: Monitorear todos los pools con los que se está trabajando.

Paso 5: Cuando el tiempo de generación en el pool sobrepasa al promedio más la desviación estándar, se calcula los tiempos y las desviaciones para los demás pools.

Paso 6: El pool cuyo tiempo de actual se acerque más al promedio y además tenga la desviación estándar más pequeña respecto a su promedio será el elegido para realizar el salto.

Paso 7: Saltar al Pool elegido en el Paso 6.

Paso 8: Volver al paso 4.

En el siguiente diagrama de flujo (ver Figura 20) se observa sistemáticamente el funcionamiento del algoritmo.

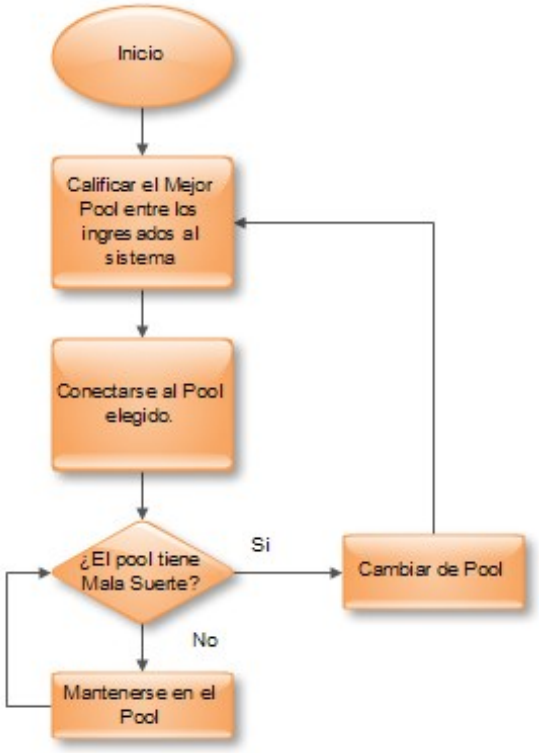


Figura 20 Diagrama de Flujo del Algoritmo

3.2. DESCRIPCIÓN DE LOS ESCENARIOS DE PRUEBAS

Las pruebas de necesarias para verificar el funcionamiento del algoritmo se realizaron en 3 escenarios el primero sirvió para contrastar el desempeño del algoritmo con los escenarios 2 y 3. A continuación en las figuras expuestas se muestra los diferentes escenarios.

La Figura 20Figura 21 presenta el Escenario 1, el cual está constituido por dos pools. El usuario inicialmente accede al pool 1, y luego después de un tiempo determinado accede al pool 2. Ese tiempo determinado es establecido como un día, que es un tiempo suficiente para obtener resultados confiables. Se aclara que el pool 1 se refiere al Slush Pool, y el pool 2 se refiere al GHASH.IO pool. Se aclara que el Slush Pool es el pool con mayor trayectoria éntrelos pools existentes por ser el primero en operar, y que el GHASH.IO que al momento de realizar el experimento era el pool con mayor capacidad en la red Bitcoin. En este escenario no existe ninguna implementación nueva, simplemente se van a recolectar los datos de operación de dos pools diferentes.

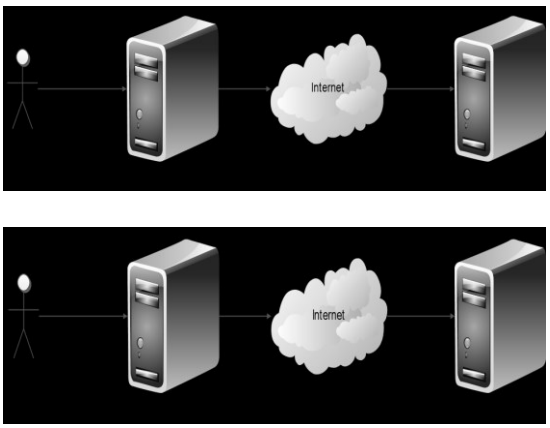


Figura 21 Escenario 1(comparación entre 2 pools al mismo tiempo)

La Figura 22 presenta el segundo escenario, el cual es constituido por los dos pools anteriormente utilizados. La diferencia es que ahora existe ya la implantación del salto automático de minería. Se van a recolectar los datos de operación en dos pools diferentes.

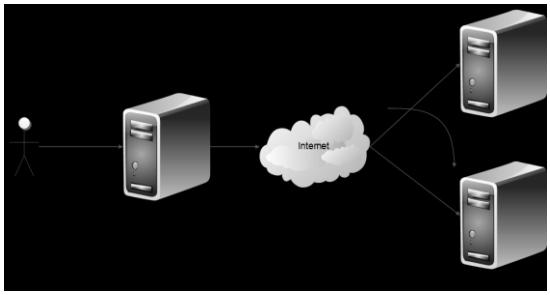


Figura 22 Escenario 2(Implementación del algoritmo de cambio de pool para dos pools).

La Figura 23 muestra el tercer escenario, el cual posee también la implantación del salto automático de minería. En este caso, se van a recolectar los datos de operación en 6 Pools diferentes.

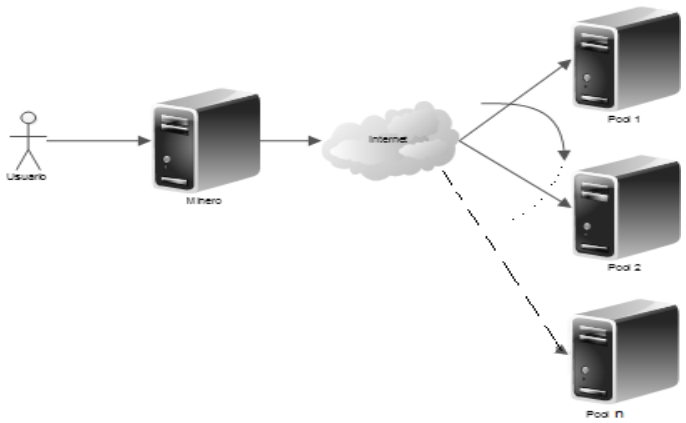


Figura 23 Escenario 3(Implementación del algoritmo de cambio de pool para n Pools)

En estos tres escenarios se usaron equipos ASIC (Aplication Specific Integrated Circuit) con una capacidad de 460GHs (giga hashes por segundo).

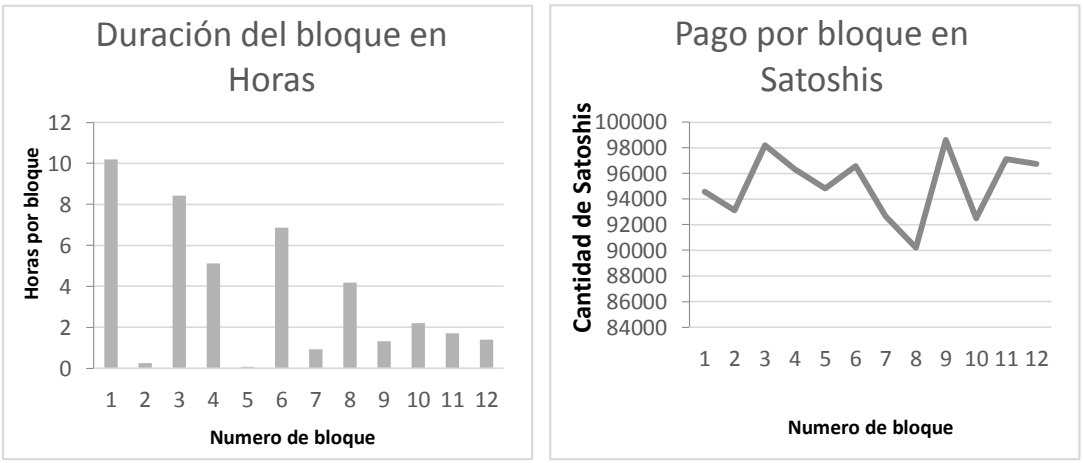
Las métricas utilizadas para analizar el algoritmo son tres: la cantidad de bitcoins generados sobre el tiempo de generación de esta cantidad en horas (rendimiento), el pago por bloque en Satoshis, y la duración del bloque. Estas tres métricas están detalladas en la Tabla 5.

Tabla 5
Métricas del algoritmo

Métrica	Definición
Duración del bloque	Es el tiempo que tardo el Pool para encontrar un bloque.
Pago por bloque en Satoshis	Es el pago que dio el Pool al encontrar un bloque, Satoshis es la unidad mínima del Bitcoin, 1 Satoshi = 0.00000001
Rendimiento	Es la cantidad en Satoshis por hora producida en los mineros en los diferentes escenarios.

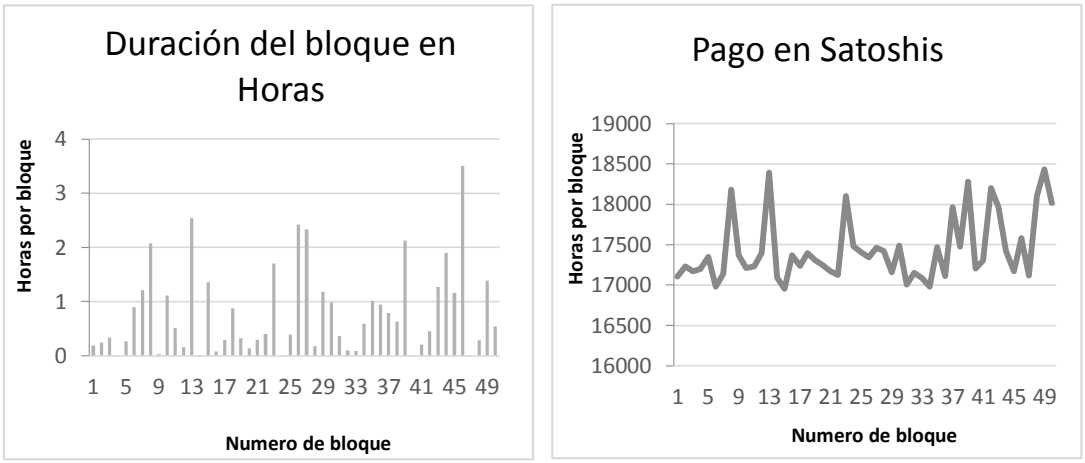
3.3. RESULTADOS

En la Figura 24 y la Figura 25 se presentan los resultados obtenidos para las métricas en el primer escenario. Por los resultados, se puede concluir que, si se mina independientemente en un solo pool, la diferencia de rendimientos entre pools no dista mucho el uno del otro. En este sentido se puede elegir cual pool es más conveniente independientemente.



(a) (b)

Figura 24 Escenario 1 en Slush Pool.- (a) Duración del bloque en horas; (b) Pago por bloque en Satoshis.



(a) (b)

Figura 25 Escenario 1 en GHash.io.- (a) Duración del bloque en horas; (b) Pago por bloque en Satoshis.

Los Rendimientos entre Pools no distan los unos de los otros esto se muestra en la Figura 26, preliminarmente se muestran los resultados de los Escenarios 2 y 3 para poder observar la diferencia entre todos los casos experimentales.

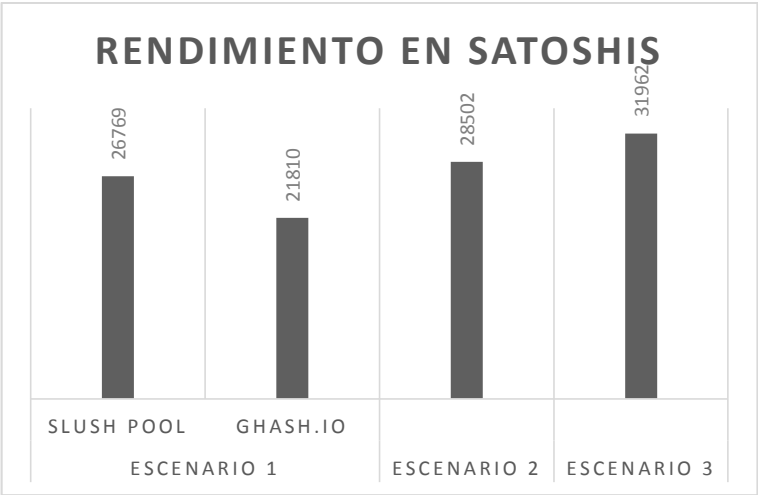


Figura 26 Rendimientos en los diferentes escenarios.

La Figura 27 y la Figura 28 presentan los resultados obtenidos para las métricas en el segundo escenario y tercer escenario respectivamente. Por los resultados, se puede concluir que se tiene una mejora significativa del rendimiento en un 7% respecto a Slush Pool y un 30% respecto a GHASH.IO. Al incrementar el número de Pools se

tiene un 12% respecto al escenario 2, un 19% respecto a Slush Pool y un 46% respecto a GHASH.IO.

Esta Diferencia es notoria en la Figura 26, a continuación se muestran los resultados individuales de los escenarios 2 y 3.

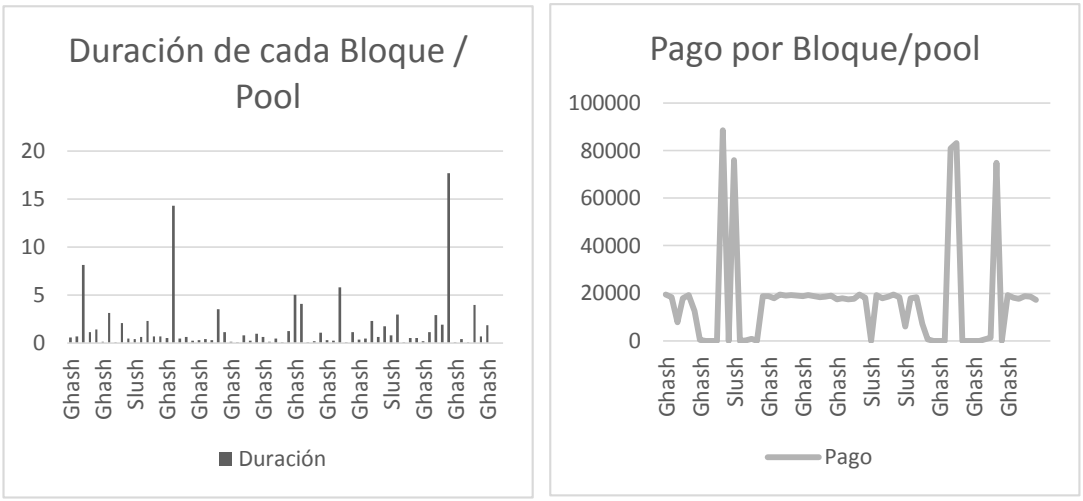


Figura 27 Escenario 2(Duración del Bloque en Horas y Pago por Bloque en Horas y por pool)

$$Rendimiento = \frac{Pago\ Total}{Horas\ Totales} = \frac{12006788}{71{,}38} = 28502\ Satoshi/Hora$$

En este escenario se puede separar los tiempos de generación entre los 2 Pools elegidos los pagos dependen del Pool elegido y de la manera como paga cada Pool.

Como se dijo antes se tiene una ventaja a minar exclusivamente en un pool.

Escenario 3:

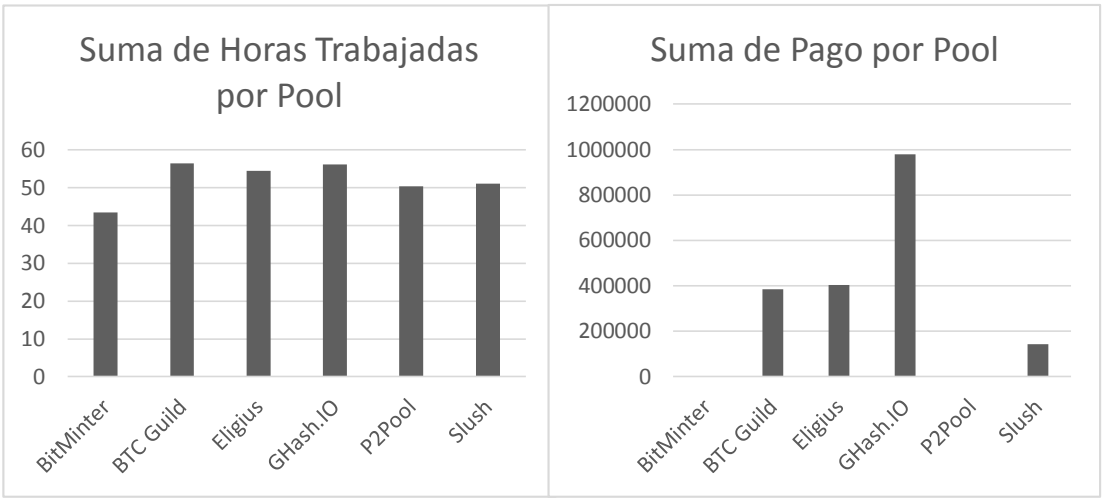


Figura 28 Escenario 3(Horas de los Bloques minados por pool y Pago por Pool)

$$Rendimiento = \frac{Pago\ Total}{Horas\ Totales} = \frac{1909122}{59.73138889} = 31962\ Satoshi/Hora$$

Las Figura 28 presentan los resultados obtenidos para las métricas en el tercero escenario. Por los resultados, se puede concluir que existe cierta preferencia a los pools que tienen mayor velocidad excluyendo a los de menor que pueden brindar un mejor rendimiento como se observa en el escenario 1. Eso puede ser un motivo de análisis para posteriores trabajos.

Por fin, observando exclusivamente la Figura 26, se puede concluir que desde el uso de 2 pools se tiene ventaja al aplicar el algoritmo de salto de pool al incrementar el número de pools con los que se trabaja se aumenta también el rendimiento sin embargo se nota claramente que se producen saltos entre los pools con mayor capacidad excluyendo a los pools de menor capacidad específicamente en el Escenario 3 se trabajó con seis pools pero solo se produjo el salto entre cuatro.

CAPÍTULO 4

DISEÑO DE POOL DESENTRALIZADO

Las aplicaciones descentralizadas se encuentran aún en el campo de la innovación, en el ecosistema de criptomonedas que existe en la actualidad, la implementación del proyecto Ethereum introdujo el concepto de contratos inteligentes, este permite brindar servicios que antes eran solo capaces por grandes corporaciones, gobiernos y notarios públicos. La importancia de este tipo de aplicaciones radica en el uso de criptomonedas, tokens o criptoacciones, estas herramientas brindan alternativas que pueden incluir a muchas más personas y equipos informáticos en su funcionamiento y manutención. (García Chávez & Da Silva Rodrigues, Automatic Hopping among Pools and Distributed Applications in the Bitcoin Network, 2016)

Lo mencionado anteriormente genera una nueva forma de generar ingresos, brindando mejores y más servicios disponibles a una creciente cantidad de usuarios.

A continuación se describen los elementos necesarios para el funcionamiento del pool.

4.1. ELEMENTOS DEL POOL

Similar a Bitcoin el pool necesita llegar a un conceso, en el caso del pool descentralizado es necesario determinar cuál es el pool idóneo para minar y entregar la capacidad de los usuarios.

Los elementos necesarios para hacer esto posible son:

- Red P2P
- Blockchain del Pool descentralizado
- Contratos Inteligentes
- Criptoacciones y/o Tokens

La red P2P y la Blockchain del pool son similares a la de una criptomoneda sin embargo se usa la estructura de P2Pool.

Las Criptoacciones son el incentivo y el mecanismo para garantizar el acceso a los otros pools, estas junto a los contratos inteligentes permiten que los usuarios del pool que van a entregar su capacidad de minería puedan asegurarse de obtener ganancias por su capacidad de generación.

Uno de los contratos necesarios es el que permita el acceso a los pools externos, su importancia radica en la dirección de la capacidad del pool, por este motivo es delicado su uso y función.

El dueño del contrato de acceso a los pools externos, debe entregar una garantía por el trabajo que va a recibir del pool en su cuenta.

En la Figura 29 Interacción de los elementos del Pool, se muestra la interacción de los elementos del pool y como estos se relacionan entre sí.

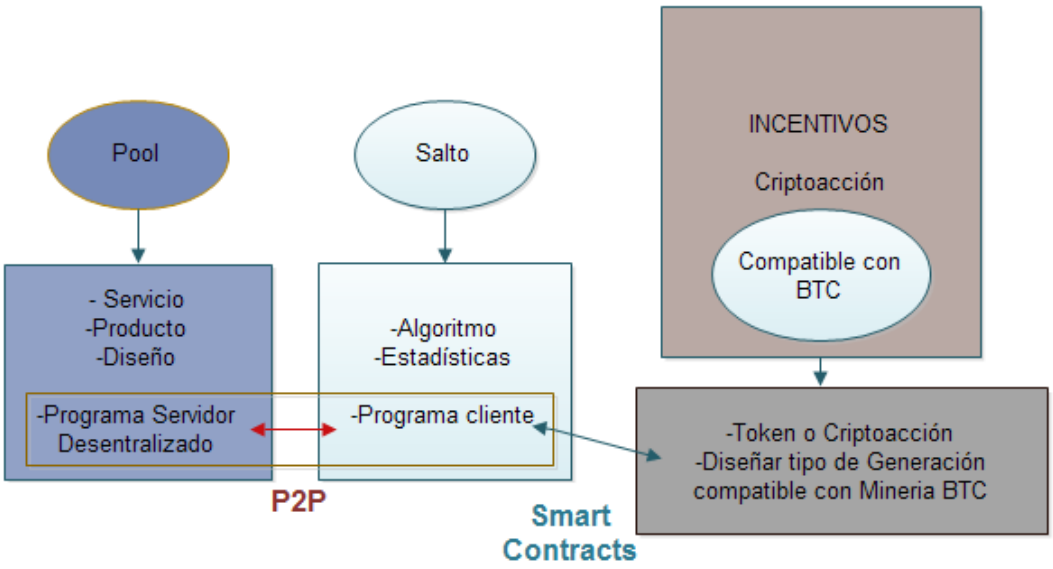


Figura 29 Interacción de los elementos del Pool

La red P2P se forma con los nodos que forman los usuarios, la aplicación también manejara los contratos inteligentes que serán los encargados de manejar los incentivos.

4.2. FUNCIONES DEL POOL

4.2.1. GESTION DE CAPACIDAD

Para gestionar de manera dinámica la capacidad que es entregada al pool los mineros pueden crear un contrato fijo o dinámico, esto permite dinamizar la capacidad entregada a pool, además de existir la capacidad de vender GHs en la plataforma a través de los contratos inteligentes.

4.2.2. ELECCIÓN Y ACCESO DE POOL EXTERNO

La elección del pool externo para minar se la realiza a través del algoritmo de salto, es importante mencionar que el acceso a los pools externos se los realiza a través de usuarios que firman un contrato inteligente garantizando la entrega de fondos al pool descentralizado.

4.2.3. MULTI CRIPTOMONEDAS

Esta Función puede ser implementada conforme se va expandiendo el pool y permite que mas mineros se incorporen a la plataforma, dinamizando así la minería de criptomonedas.

4.3. MODELO DE FUNCIONAMIENTO

El funcionamiento del Pool requiere de una aplicación que va a formar un nodo similar a los nodos de la red bitcoin para acceder al pool descentralizado y para minar.

En la Figura 30 se observa la estructura de la aplicación que permite manejar, los contratos inteligentes, el acceso al pool descentralizado y los incentivos (criptoacciones). Esta aplicación la usaran los usuarios finales por eso se lo llamara “User Pass”.

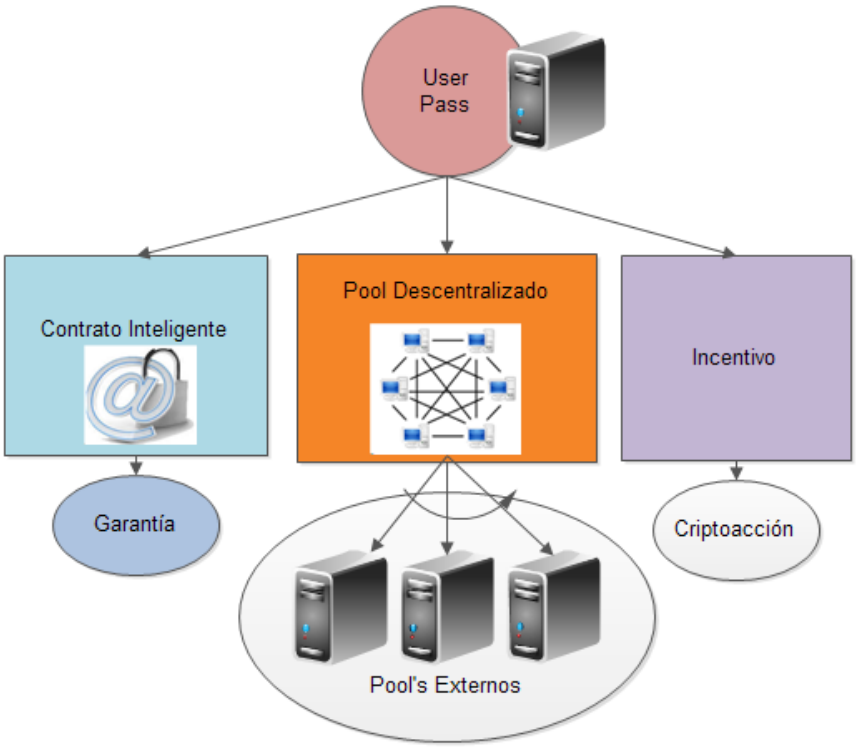


Figura 30 User Pass – Aplicación Pool Descentralizado

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Luego de una profunda investigación acerca del funcionamiento de las aplicaciones descentralizadas y como el Protocolo Bitcoin soluciona el problema de depender de una entidad central para manejar un sistema transaccional, los elementos como la cadena de bloques y los contratos inteligentes son elementos claves para avanzar en el diseño del pool descentralizado.
- El diseño de un algoritmo de salto de pool indica una ventaja sobre minería de bitcoin tradicional, esto es observado claramente en los resultados los cuales incrementan en hasta un 46% respecto a minar en un único pool.
- Con los nuevos tipos de implementaciones de contratos inteligentes se crean posibilidades de construir plataformas descentralizadas para diferentes aplicaciones, una potencial es el desarrollo del pool descentralizado que se expone en este trabajo y es importante por los diferentes tipos de incentivos que se podrían generar en la plataforma.
- La integración del algoritmo desarrollado junto con los elementos de las aplicaciones descentralizadas que usan la tecnología introducida por el protocolo Bitcoin permiten el diseño presentado en este trabajo de investigación.

5.2. RECOMENDACIONES

- Para la futura implementación del diseño expuesto se requiere que el algoritmo propuesto se emplee como una línea de base sólida para desarrollar otras propuestas dirigidas a un uso aún más eficiente entre pools, considerando otros aspectos técnicos diferentes. Por ejemplo, las redes P2P demandan más participantes para tener más fiabilidad y estabilidad, se modificar el algoritmo

propuesto para incluir grupos de menor capacidad podría optimizar el rendimiento general de la plataforma.

- Adicionalmente, se podrían incluir otros puntos de discusión para análisis adicionales: (1) cálculo de estimadores robustos que no sean la media y la desviación estándar, tales como la mediana y los intervalos de generación; (2) comparación de desempeño entre la tasa media del pool y la tasa promedio general (conjunto de pools); Por último, (3) una explicación detallada del hardware relativo a los ASIC, incluso desarrollando ASIC más generales para aumentar las criptomonedas participantes de la plataforma.

BIBLIOGRAFÍA

A.Back. (2012). *Hashcash - A Denial of Service Counter- Measure*. Obtenido de www.hashcash.org

Antonopoulos, A. (2014). Mastering Bitcoin. *O'Reilly 2da edi*.

Bitcoin Network Graphs. (18 de 12 de 2016). Obtenido de http://bitcoin.sipa.be/speed-lin-ever.png

Blair, G. C. (s.f.). Distributed Systems – Consepts and Design. 423-461.

Edward, J. A. (2013). The Economics of Bitcoin Mining or Bitcoin in the Presence of Adversaries. *Workshop on the Economics of Information Security*.

Ethereum community. (2016). *Ethereum Homestead Documentation*. Recuperado el 2016, de http://www.ethdocs.org/en/latest/

F. Reid, M. (2011). An Analysis of Anonymity in the Bitcoin System. *1st Workshop on Security and Privacy in Social Networks (SPSN'11) at SocialCom 11 IEEE.*

García Chávez, J. J., & Da Silva Rodrigues, C. K. (2015). A simple algorithm for automatic hopping among pools in Bitcoin mining network. *The SIJ Transactions on Computer Networks & Communication Engineering, v. 3*, 22-27.

García Chávez, J. J., & Da Silva Rodrigues, C. K. (2016). Automatic Hopping among Pools and Distributed Applications in the Bitcoin Network. *IEEE Xplore*.

Herrera-Joancomart, J. A.-S. (2014). The Bitcoin P2P Network. *Financial Cryptography and Data Security, Vol. 8437*, 87-102.

Lerner, S. D. (2015, Nov 19). (R. B. Contracts, Ed.) Retrieved from http://www.rsk.co/

Nakamoto, S. (2008). *Bitcoin: A peer – to – peer electronic cash system*. Recuperado el 2016, de http://www.bitcoin.org/bitcoin.pdf.

Page, The International PGP Home. (16 de 12 de 2016). *How PGP works - The Basics of Cryptography*. Obtenido de http://www.pgpi.org/doc/pgpintro/

Palatinus, M. (2010). *Slush Pool*. Recuperado el 2016, de http://mining.bitcoin.cz/.

Rubin, I. M. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *Security and Privacy (SP) 2013 IEEE Symposium on*, 397–411.

Sirer, I. E. (2013). Majority is not enough: Bitcoin Mining is Vulnerable. *Financial Cryptography and Data Security, Vol. 7859*, 436-454.

Smith, J. (2013). *GHASH.IO*. Recuperado el 2016, de https://ghash.io/.

Stevens, R. (2012). *TCP/IP Ilustrated.* Upper Saddle River, NJ: Pearson Education, Inc.

Uzun, S. B. (2012). Bitter to Better - How to Make Bitcoin a Better Currency. *Financial Cryptography and Data Security - 16th International Conference*, 397-414.

Welten, T. B. (2013). Have a snack, pay with Bitcoins. *Peer-to-Peer Computing (P2P) IEEE Thirteenth International Conference on*.

Wood, G. (2015). Ethereum: A secure decentralised generalised transaction ledger. *Homestead Revision*, http://gavwood.com/paper.pdf.