Análisis Y Comparación De Monedas Criptográficas Basadas En La Tecnología Blockchain

Maria Fernanda Medina Reyes

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Jordi Herrera Joancomartí

Universidad Autónoma de Barcelona

13/06/2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	Análisis y comparación de monedas criptográficas basadas en la tecnología blockchain
Nombre del autor:	Maria Fernanda Medina Reyes
Nombre del consultor:	Jordi Herrera Joancomartí
Fecha de entrega (mm/aaaa):	06/2016
Área del Trabajo Final:	Seguridad en servicios y aplicaciones - Criptografía
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo

Bitcoin es la primera implementación de moneda digital que ha sido capaz de abordar eficazmente el problema de doble gasto (que permite pasar una moneda digital dos veces). Al ser un proyecto de código abierto, el estudio y análisis de Bitcoin ha traído una colección de nuevas propuestas de cambio de cifrado inclusive, denominas Altcoins o monedas alternativas, tales como: Bytecoin, Litecoin, Dogecoin, Verge, Syscoin, Digibyte, entre otras.

Como propósito central del trabajo se ha creado un informe actualizado de las propuestas más relevantes. La información es categorizada y se analiza las criptomonedas dependiendo las principales propiedades proporcionando datos sobre sus similitudes y diferencias, al igual de cómo es su comportamiento al momento de hacer transacciones con cada una de ellas.

Abstract:

Bitcoin is the first digital currency implementation that has been able to deal eficiently with the problem of double spending (which allows to spend a digital coin twice). Being an open source project, bitcoin study and analysis has brought a collection of new crypto currency proposals, denominated altcoins like Bytecoin, Litecoin, Dogecoin, Verge, Syscoin, Digibyte, among others.

The goal of this project is to create an up to date report of the most relevant crypto currency proposals. Information is categorized and analyzed currencies depending on their main properties and provide a comprehensive information on their similarities and differences, as performance like transactions with each of them.

Palabras clave:

Bitcoin, Criptomonedas, Cadena de bloques, Prueba de trabajo

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

Hacer un estudio comparativo entre las diferentes criptomonedas que existen actualmente puede resultar complejo y muy disperso al momento de elegir las características o propiedades que se desean comparar. No hay una norma, regla o metodología definida al hacer comparativas entre criptomonedas a priori, el tema se ha venido trabajando recientemente y la información está muy dispersa, en la actualidad se han venido desarrollando y trabajando nuevas criptomonedas, coexistiendo hoy por hoy más de 624 aprox [1] , por lo cual se busca establecer un punto de comparación entre algunas de ellas.

Por ello, centrarse en el bitcoin como base es el primer paso, así, tomando como referencia ésta criptomoneda se puede realizar comparativas a muchos niveles. En el presente trabajo se pretende abarcar y centrar las características y propiedades de las monedas que trabajen con pruebas de trabajo (Proof – Of – Work, POW) como sistema de minado y las que estén basadas en la tecnología de cadenas de bloques (Block – Chain), se busca estudiarlas siguientes propiedades: Sistema utilizado para incluir bloques en la cadena, es decir distinguirlas en función del POW que se utiliza (SHA-256, Scrypt, etc.), el sistema de distribución de la moneda con respecto al volumen de monedas que se van generando, características de los bloques, rendimiento de las transacciones por unidad de tiempo, plataformas disponibles en la que los usuarios puedan hacer diferentes funciones como la minería y la seguridad de bloques transaccionales.

1.2 Objetivos del Trabajo

1.2.1 Objetivo General

Establecer criterios de comparación de las diferentes criptomonedas, en cuanto sus características.

1.2.2 Objetivos Específicos

- Seleccionar las monedas criptográficas basadas en la tecnología block-chain y en su capitalización que serán tenidas en cuenta en el estudio.

- Categorizar las criptomonedas seleccionadas en función de sus principales propiedades, con el fin de proporcionar una amplia información sobre sus similitudes y diferencias.

- Describir el proceso de minado de cada criptomoneda que utilice Proof of Work, a fin de establecer similitudes y diferencias significativas entre cada criptomoneda incluyendo un análisis de seguridad de cada una.

- Crear un reporte actualizado de las propuestas de monedas criptográficas más relevantes seleccionadas, categorizando cada criptomoneda en función de sus propiedades, proporcionando una amplia información sobre sus similitudes y diferencias y el cómo es afectada su seguridad.

1.3 Enfoque y método seguido

En la primera parte del trabajo se realizará una revisión del funcionamiento de la moneda criptográfica, se desplegarán las características básicas de las criptomonedas y se estudiará en detalle el funcionamiento de los bitcoins como base de las distintas monedas seleccionadas.

Tomando como base las características básicas revisadas de las criptomonedas, se determinará una metodología apropiada que permita establecer parámetros de comparación entre las criptomonedas en cuanto a sus características principales y propiedades, en esta parte se definirá en que consiste cada característica seleccionada, tales como: El sistema utilizado para incluir bloques en la cadena, los mecanismos de autenticación, el sistema de distribución de la moneda con respecto al volumen de monedas que se van generando, características de los bloques y el rendimiento de las transacciones por unidad de tiempo, las plataformas disponibles en la que los usuarios pueden hacer diferentes funciones como lo es la minería por ejemplo, y por último revisar la seguridad de las cadenas de bloques transaccionales.

Una vez definidas las características básicas de las criptomonedas se procede con la clasificación de cada una de ellas. El trabajo se limitará a las monedas que trabajen con el sistema Proof-of-Work, POW) y que están basadas en la tecnología de cadenas de bloques (block-chain). Las monedas seleccionadas a parte del Bitcoin son 6 y han sido escogidas en función de su capitalización de la siguiente forma: Más de 2 millones de dólares: Bytecoin (BCN) y Litecoin (LTC) y Dogecoin (DOGE); con capitalización entre 1 y 2 millones: Verge (XVG), SysCoin (SYS) y DigiByte (DGB).

En esta última parte con base a la metodología seleccionada se generará un informe actualizado donde se dará un criterio de comparación y medición de cada moneda en función de las propiedades anteriormente seleccionadas y descritas.

1.4 Planificación del Trabajo

			Febrero	Marzo	Abril			Mayo				Junio		
Actividad			24-feb	14-mar	01-abr	18-abr	24-abr	01-may	08-may	15-may	27-may	05-jun	13-jun	17-jun
Desarrollo de la propuesta del proyecto	24-feb	14-mar												
Seleccionar las monedas	14-mar	18-abr												
Revisar el funcionamiento de la moneda criptográfica	14-mar	18-abr												
Detallar el funcionamiento de los bitcoins	14-mar	24-abr												
categorizar las monedas seleccionadas	18-abr	24-abr												
Comparar y medir características de cada moneda	24-abr	27-may												
Crear memoria y producto resultante	27-may	13-jun												
Inicio fase final	05-jun	17-jun												

1.5 Breve descripción de los otros capítulos de la memoria

En este trabajo se han desarrollado los siguientes capítulos, encaminando al resultado de los objetivos propuestos.

En el capítulo 2 “Introducción a las criptomonedas”, se hace referencia a las criptomonedas y cada una de sus propiedades.

En el capítulo 3 “Descripción de las criptomonedas “, se describe con detalle cada una de las características y propiedades que tienen las criptomonedas que se han seleccionado

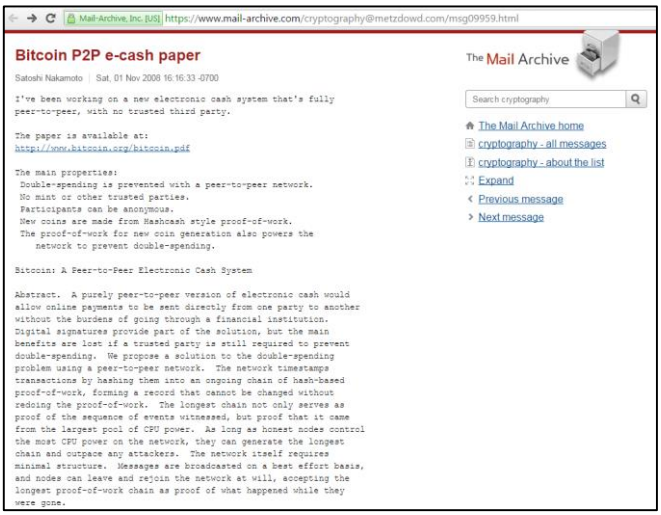
En el capítulo 4 “Comparativa entre las monedas” y último capítulo, se establecen las comparaciones entre cada criptomoneda y se evalúa a nivel de bloques la relación entre ellas.

2. Capítulo 2 – Introducción a las criptomonedas

2.1 Definición Bitcoin

Bitcoin es una moneda digital descentralizada sin una autoridad central o intermediarios, la cual es impulsada por sus usuarios, funciona bajo el concepto de “Moneda Criptográfica”, concepto que fue descrito por primera vez en 1998 por Wei Dai en la lista de correo electrónico "Cypherpunks[1]", donde propuso la idea de un nuevo tipo de dinero que usará la criptografía para controlar la creación y las transacciones, en lugar de una autoridad centralizada. [2] . Cypherpunks fue el predecesor de donde Satoshi Nakamoto anunciaría al mundo el Bitcoin.

En 2008, Satoshi Nakamoto publicó en la lista de correo la primera especificación del protocolo de red de Bitcoin junto con la prueba de concepto y en 2010 abandonó el proyecto sin revelar su identidad, desde entonces la comunidad ha crecido en forma exponencial y diferentes comunidades de desarrolladores que trabajan en el protocolo.


Mail-Archive, Inc. [US] https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

The Mail Archive

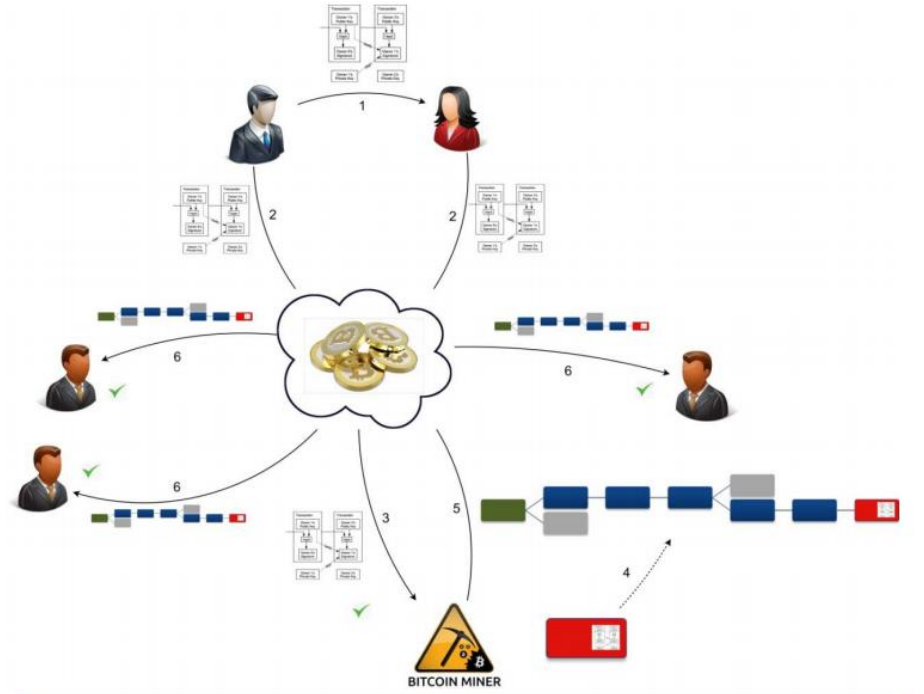
Search cryptography

The Mail Archive home
cryptography - all messages
cryptography - about the list
Expand
Previous message
Next message

Ilustración 1. Mensaje de Satoshi Nakamoto en la lista de correos [3]

Los bitcoins se crean mediante un proceso llamado minería, que se basa en encontrar soluciones a un problema matemático donde a su vez se procesan transacciones bitcoin, cada 10 minutos en promedio se consigue verificar y registrar transacciones las cuales son recompensadas con nuevos bitcoins. El protocolo bitcoin incluye algoritmos que regulan la función de minería en toda la red.

[1] El termino Cypherpunk hace referencia a activistas que abogan por el uso generalizado de encriptación como medio para cambios sociales y políticos, con el objetivo de alcanzar la privacidad y seguridad mediante el uso de la criptografía. Lleva activo desde finales de los 80.



1. *Bob hace un pago en bitcoins a Alice.*
2. *Alice y Bob envían la transacción a la red P2P de Bitcoin.*
3. *Un minero recibe la nueva transacción y la verifica.*
4. *El minero crea un conjunto de transacciones nuevas, incluyendo la transacción del paso 1, y trabaja para confirmarla.*
5. *El minero envía el nuevo bloque de transacciones confirmadas a la red P2P de Bitcoin.*
6. *El resto de usuarios de Bitcoin actualizan su estado incluyendo el nuevo bloque de transacciones, verificando que dicho bloque es válido.*

Ilustración 2. Funcionamiento genérico de un Bitcoin [4]

Para registrar con éxito un bloque de transacciones “Block-chain” se ajusta dinámicamente de forma que, en promedio alguien será exitoso cada 10 minutos (entiéndase a alguien como una persona, CPUs, equipos avanzados, etc.) sin importar cuántos mineros hayan trabajado en la tarea en cada momento. El valor límite es de 21 millones de monedas. Se prevé que el número de bitcoins en circulación alcance su límite en el año 2140 en cual llegaría a 20,999,999.9769 BTC, debido a que su circulación sigue una curva predecible [5].

2.2 Función hash criptográfica

Las funciones hash criptográficas son funciones hash que se usan en muchos algoritmos y protocolos criptográficos, existen muchas aplicaciones en el área de la seguridad de la información, algunos de los algoritmos más comunes en esta categoría incluyen algoritmos como el SHA-256, que en realidad es procedente de SHA-1 y así. También existen otros algoritmos como RIPEMD, BLAKE, Skein, entre otros.
Históricamente las aplicaciones de este tipo de funciones hash fue en el contexto de las firmas digitales, las cuales son usadas en muchas diferentes aplicaciones hoy día como pilar fundamental de muchos protocolos e-commerce. Las funciones hash criptográficas también son usadas para generar mensajes de autenticación de protocolos con la generación de números aleatorios y contraseñas de seguridad, se caracteriza por reducir el mensaje

original a una secuencia de bits que lo identifica y que se denomina “huella digital (Fingerprint)” o “compendio (Digest)” del mensaje.

Los algoritmos (Fingerprint o Message Digest) realizan operaciones matemáticas sobre el mensaje original para calcular un valor de tamaño fijo (de 128, 160, 256, 384 o 512 bits), es decir, la huella digital.

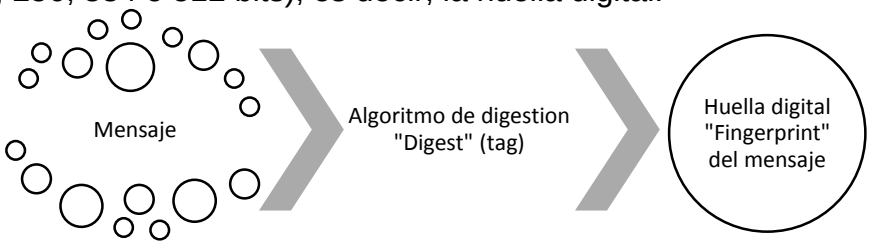


Ilustración 3. Firma digital

Se utiliza una función de dispersión unidireccional (de un solo sentido, es decir, no se puede reconstruir el mensaje a partir de su “compendio” o “huella digital”) que cumple una serie de propiedades criptográficas como:

- Eficiencia computacional, no debe tomar mucho tiempo calcular la salida de una entrada

- Al conocer la “huella digital” no se obtiene ninguna información sobre el mensaje original

- No es factible encontrar dos mensajes originales (inputs) que generen la misma “huella digital” La probabilidad de colisión, de la misma secuencia de bits a partir de dos mensajes distintos, es muy remota, prácticamente nula. Esto se le denomina “Collision resistance”.

- Un cambio cualquiera en el mensaje de entrada debe modificar, en promedio, la mitad de los bits que se generan a la salida del algoritmo, es decir, un pequeño cambio en el mensaje cambia totalmente su huella digital.

Los algoritmos MD4 (1990) y MD5 (1992), diseñados por Ron Rivest, generan compendios de 128 bits (estos algoritmos no se utilizán puesto que se consideran inseguros). A su vez, el algoritmo SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) fue desarrollado por el NIST (National Institute of Standards and Technology) para generar compendios de 160 bits. El algoritmo SHA-1 es una revisión técnica de SHA realizada en el año 1995.

2.3 Firmas Digitales

La firma electrónica son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los datos así como protegerlos contra falsificaciones. (Definición de la ISO 7498-2).

Para entender el concepto de firma digital es necesario entender que es un criptosistema de clave pública. Las firmas digitales más utilizadas actualmente son: RSA, ElGamal y Digital Signature Standard (DSS). Y por último es necesario entender el concepto de función Hash.

Para su obtención, se sigue un esquema bastante sencillo; el creador de un mensaje debe cifrar la “huella digital” del mensaje con su clave privada y enviarla al destinatario acompañado al mensaje cifrado. El cifrado asimétrico (mediante un algoritmo como RSA) se aplica sobre la “huella digital” del mensaje y no sobre el propio mensaje, debido al elevado coste computacional que supondría el cifrado de todo el mensaje, ya que esta alternativa resultaría mucho más lenta compleja.

Ilustración 4. Obtención de la firma digital de un mensaje

En la siguiente figura se muestra el procedimiento seguido por un usuario A para enviar un mensaje cifrado a otro usuario B acompañado de la correspondiente firma electrónica:

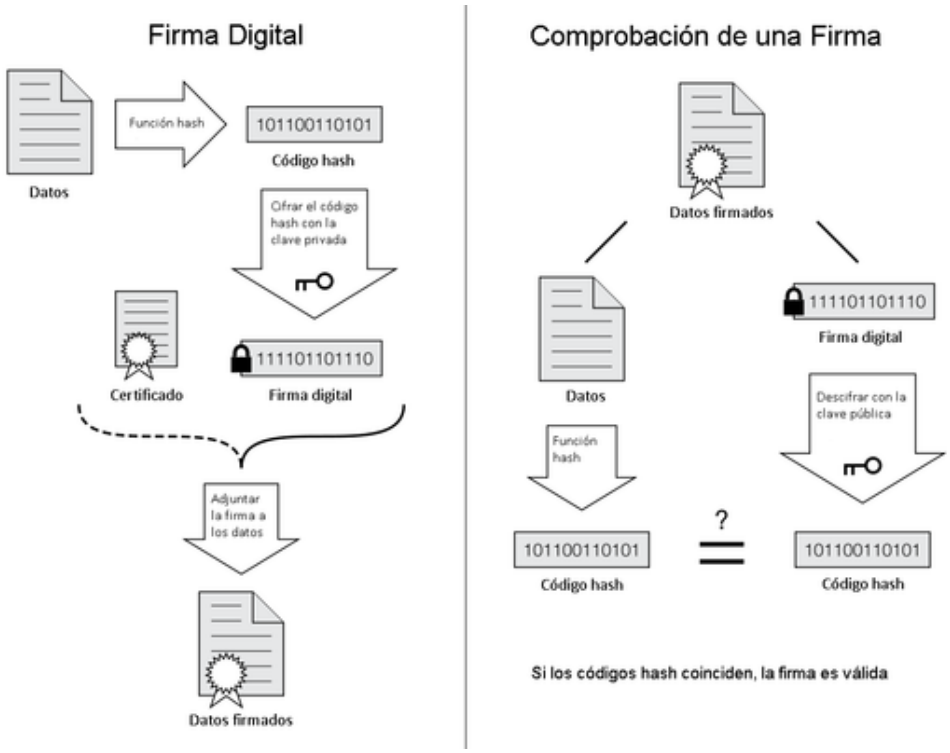


Ilustración 5. Proceso Firma digital

2.3.1 SHA-256

El SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y

Tecnología (NIST) Registro de transacciones. SHA es una de las muchas funciones hash como una firma para un texto o fichero, es de 64 dígitos hexadecimales (Ej.: “maria” = 94-ae-c9-fb-ed-98-9e-ce-18-9a-7e-17-2c-9c-f4-16-69-05-04-95-15-2b-c4-c1-db-f2-a3-8d-7f-d8-56-27) casi único de tamaño fijo de 256 bits (32 bytes). Un hash solo se calcula en una dirección y no se puede decodificar de vuelta.

El primer miembro de la familia fue publicado en 1993 y es oficialmente llamado SHA, sin embargo hoy día se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde aparece SHA-1, y existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384 y SHA-512 (denominándose SHA-2 a todos ellos). [6].

Uno de los algoritmos criptográficos más comunes cuando se estudia el protocolo Bitcoin es SHA-256, se utiliza en la creación de claves o direcciones públicas y en la minería de Bitcoin. Fue la primera criptomoneda que utilizó SHA-2 como parte de su esquema de prueba de trabajo “Proof-of-work”. En los cálculos de hashes realizados en Bitcoin se utilizan los estándares SHA-256 y, cuando se requiere que el hash sea más corto, RIPEMD-160. Normalmente el cálculo de hashes se realiza en dos fases: La primera con SHA-256 y la segunda, dependiendo de las necesidades de longitud del resultado, con SHA-256 o RIPEMD-160.

Ejemplo:

```
SHA-256("Hola") = E6 33 F4 FC 79 BA DE A1 DC 5D B9 70 CF 39 7C
82 48 BA C4 7C C3 AC F9 91 5B A6 0B 5D 76 B0 E8 8F

SHA-256(SHA-256("Hola")) = A7 53 96 6A 11 02 90 57 D6 50 C4 C3
0C 2E 3F 52 8A B6 83 8B 96 C7 BA BB 74 3A EB 9E 3D 6B C4 01

RIPEMD-160(SHA-256("Hola")) = F9 3B 68 56 C7 BD 9F 91 97 F7 B5
0F 35 93 09 EE 98 80 92 41
```

El proceso de creación de una dirección pública de Bitcoin se inicia con un par de claves privada y pública de una curva elíptica ECDSA. Las direcciones públicas que se ve cuando se usa un cliente monedero “wallet” Bitcoin ha pasado por un proceso de creación de clave pública y hashing en el que se utilizan las funciones hash SHA-256 y RIPEMD-160 para maximizar su seguridad. Como en el ejemplo anterior.

2.3.2 Curva elíptica ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm - Algoritmo de Firma Digital de Curva Elíptica), es una variante del Digital Signature Algorithm (DSA) que utiliza la criptografía de curva elíptica (Elliptic curve cryptography – ECC) como variante de la criptografía asimétrica o de clave pública. La criptografía de curva elíptica puede ser más rápida y usar claves más cortas que los métodos antiguos como RSA, al tiempo que proporciona un nivel de seguridad superior [7] [4].

Las ventajas que ofrece ECDSA frente a otros esquemas de firma que lo hacen ideal para su utilización en un protocolo distribuido en internet como:
- Longitudes de clave y de firma muy cortas: Los primeros algoritmos criptográficos de clave pública se basaban en la factorización de números primos grandes (Ejemplo: RSA[2], el cual basa su seguridad en el problema de la factorización de números enteros. Los mensajes se representan mediante números, y el funcionamiento se basa en el producto, conocido de dos números primos grandes elegidos al azar y mantenidos en secreto), estos algoritmos ya no se consideran seguros cuando se utilizan claves cortas, la criptografía de curva elíptica genera claves "intractable" en inglés, que traducido al español significa "difícil de resolver" pero no imposible.

- Generación y verificación de firmas muy rápidas: crear claves más pequeñas, reduciendo así requisitos de almacenamiento y transmisión.

2.6 Prueba de trabajo

Proof of work, en inglés, son el principal componente de Bitcoin responsable de garantizar que la red mantiene un comportamiento legítimo. La creación PoW puede representar el proceso casual con una pequeña probabilidad de éxito, bitcoin usa así "Hashcash", una función para la ejecución de la prueba de trabajo (PoW).
El uso de Hashcash sirve para la prevención del spam de correo electrónico, requiriendo una prueba de trabajo en el contenido del email (incluyendo la dirección) de cada correo. Los correos electrónicos legítimos serán capaces de hacer el trabajo para generar la prueba con facilidad (no se requiere mucho trabajo para un solo correo electrónico), pero los que envían correos de spam masa tendrán dificultades para generar las pruebas necesarias (lo que requeriría enormes recursos computacionales). [8].
La prueba de trabajo consiste en calcular el hash (SHA-256) de los seis valores de la cabecera. El hash resultante debe ser menor que el número codificado en Bits.

2.7 Bloques

Son registros que contienen confirmaciones de transacciones que se encuentran pendientes. Aproximadamente cada 10 minutos, en promedio, aparece un nuevo bloque que incluye nuevas transacciones que a la vez se guardan en forma cronológica en una cadena de bloques llamada "block-chain". Es normal esperar que una transacción obtenga hasta 6 confirmaciones (1 hora) para ser considerada válida, si bien este tiempo es variable y puede depender del vendedor y de la cantidad monetaria. Estos nodos que verifican y agregan transacciones son los nodos mineros.

Los campos de un bloque son:
- Magic no: Valor establecido siempre (0xD9B4BEF9)

[2] RSA – (Rivest Shamir y Adlean los creadores). Es un sistema criptográfico de clave pública desarrollado en 1977, es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

- Blocksize: Número de bytes que siguen, hasta el final del bloque
- Blockheader: Cabecera con metainformación sobre el bloque y la cadena
- Transaction counter: Numero de transacciones en la siguiente lista
- Transactions: Lista de transacciones contenidas en el bloque

La cabecera del bloque contiene:

- Version: Versión del bloque
- HashPrevBlock: Hash del bloque anterior
- HashMerkletRoot: Hash raíz del árbol Merkle
- Time: Marca de tiempo de creación del bloque
- Bits: Especificación de la complejidad del bloque
- Nonce: Nonce que resuelve la prueba de trabajo, es el número que resuelve la prueba de trabajo.

2.8 Cadena de bloques – Blockchain

Blockchain o cadena de bloques son registros públicos de transacciones de Bitcoins que están validadas en orden cronológico, de tal forma que cada vez que un bloque es confirmado pasa a ser parte de la cadena. El primer registro se hizo el 3 de enero de 2009, a partir de aquí en orden cronológico cuando un nodo de la red consigue crear un nuevo bloque, éste lo transmite al resto de nodos, los cuales verifican que el bloque es correcto, en caso que se confirme, se añade a la cadena y se difunde, se asegura la seguridad porque todas las transacciones son públicas y difícil de falsificar, automatizado por algoritmos matemáticos en la cual la comunidad puede hacer de 'notarios' que certifican el documento.

Un usuario no puede reutilizar monedas que ya usó, puesto que la red rechazará la transacción porque éstas transacciones se hacen públicas, imposibilitando una reutilización, de hecho, en la página de Blockchain se puede observar casos de reutilización de monedas que se han detectado y bloqueado.

El blockchain es creado por el minero y mantenido por el resto de usuarios, el minero envía un bloque de transacciones confirmadas a la red peer to peer (p2p) de Bitcoin, el resto de usuarios actualizan su estado incluyendo el nuevo bloque de transacciones verificando que dicho bloque es válido.

Un blockchain se construye de la siguiente forma:

Cada vez que se hace una transferencia de una dirección bitcoin a otra, el propietario de la dirección origen firma una transcripción de la dirección destino, esto crea una estructura que contiene tanto claves como otros datos, los cuales están pendientes de confirmar, estos datos se agrupan en bloques, entonces sobre cada bloque se realiza la minería, una vez validados y confirmados estos pasan a formar parte de la cadena denominada blockchain.

El tiempo medio de generación de un bloque es de 10 minutos, actualmente, según Blockchain.info [9] es de 8.78 minutos, por defecto cada cliente debería esperar 6 bloques, es decir, hasta que no se hayan validado 6 bloques desde

que se comenzó la transacción, porque de lo contrario no se considera realmente efectuado el pago. Por otro lado, la red trata de crear 6 bloques por hora, y cada 2016 bloques (Aprox. dos semanas), todos los clientes comparan el número real creado con este objetivo y modifican el porcentaje que ha variado, lo cual aumenta (o disminuye) la dificultad de generación de bloques. [10].

2.9 Proceso de creación de una clave pública Bitcoin

Una dirección en la red Bitcoin se compone de dos claves, una pública y otra privada, la dirección se identifica con el hash de la clave pública a la cual se añade una suma de verificación, éste resumen se codifica en una versión modificada de base 58, manteniendo los ceros a la izquierda cuando se realiza la codificación. Tomando la siguiente forma:

```
$Version = 1 byte de ceros
$KeyHash = $Version + RIPEMD-160(SHA-256($PublicKey)
$Checksum = SHA-256(SHA-256($KeyHash))[0-3]
$BitcoinAddress = Base58Encode($KeyHash + $Checksum)
```

Todas las operaciones que se realizan con esa dirección (de la clave pública) deben estar apoyadas por la utilización de la clave privada asociada, es decir, firmadas, por lo tanto únicamente al usuario puede utilizar los bitcoins [4].

2.10 Transacciones por segundo

Las transacciones en las criptomonedas se hacen entre billeteras (wallets), no entre personas y se hacen por segundo, denominadas transactions per second en inglés o TPS.

Para calcular aproximadamente la TPS de una moneda se necesita conocer el número total de transacciones y el tiempo en el que se llevaron a cabo. Para el caso de las criptomonedas está:

$$\frac{Block\ Size\ Limit}{Lowest\ possible\ tx\ size * Block\ time\ in\ seconds}$$

3. Capítulo 3. Descripción de las criptomonedas

El primer criterio al momento de seleccionar las criptomonedas a trabajar es de acuerdo a su capitalización: Con capitalización de más de 2 millones de dólares: Bitcoin (BTC), Bytecoin (BCN), Litecoin (LTC) y Dogecoin (DOGE) y Capitalización entre 1 y 2 millones: Verge (XVG), Syscoin (SYS) y DigiByte (DGB). A continuación se muestra un resumen obtenido de coinwarz.com [11], la última fecha de consulta fue *27 de Mayo de 2016.*

3.1 Bitcoin (BTC)

Como se ha definido en el apartado 2.2, Bitcoin fue la primera criptomoneda que comenzó a operar en el año 2009 y desde entonces se han creado muchas otras, denominadas altcoins.

3.1.1 Especificaciones

- Algoritmo usado: SHA-256

- Cada confirmación esta entre pocos segundos y 90 minutos máximo, con 10 minutos siendo el promedio entre transacciones. Si la transacción paga una tasa muy baja o es de otra manera atípica, conseguir la primera confirmación puede tomar mucho más tiempo. Cada usuario es libre de determinar en qué momento se considera una transacción totalmente confirmada, pero 6 confirmaciones se considera a menudo ser tan seguro como esperar 6 meses en una transacción con tarjeta de crédito

- Velocidad de Hash: Cuando alcanza 10 TH/s, 10 billones de cálculos por segundo

- Moneda divisible 8 decimales, y cada unidad decimal es denominada Satoshi, 0.00000001 BTC es la unidad minima.

- Bloque génesis: genex - {'date': 1231006505, 'magicbytes': 'f9beb4d9', 'name': 'Bitcoin', 'starting_difficulty': 'f9beb4d9', 'merkle_root': '**4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b**', 'port': 8333}

- Tamaño máximo bloque (Maximum block size): 1MB

- Promedio de tamaños de bloques: (Junio 2016) 798,470 bytes = 0.79847 MB [12], sin embargo se tomaran los valores entre 250 bytes y 500 bytes para hacer los cálculos comparativos entre las demás monedas, estos tamaños son tomados del paper del IC3 [13], cuyas transacciones por segundo están entre 3.3 y 7 TPS.

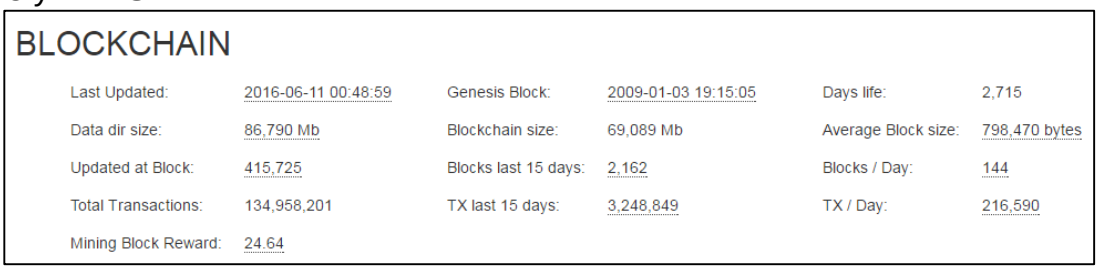


Ilustración 6. BlockChain Junio 2016 BITCOIN [12]

3.1.2 Información de la moneda

Bitcoin Price	$475.59 USD per BTC **
Fecha Bloque Genesis	Friday, January 09, 2009 02:54:25 GMT
Icono	
Nombre	Bitcoin
Simbolo / Etiqueta	BTC
Website (Descarga Bitcoin Wallet)	https://bitcoin.org
Github / Código Fuente	Github (https://github.com/bitcoin/bitcoin)
Foro	Bitcointalk (https://bitcointalk.org/)

Bitcoin Wallet Version (Client Version)	v0.12.0 Get Info RPC Version: 120000	Protocol Version: 70012 Wallet Version: 60000
Status	Healthy	
Connections	8	
Algoritmo Hash	SHA-256	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	21,000,000	
Tiempo generación bloque	10.00 minutos	
Recompensa por bloque	25.00 coins	
Block Count	413,679	
Bitcoin Difficulty	199312067531.243	
Difficulty Retarget	2,016 blocks	

**** Bitcoin Price** está basado en el precio más alto a la fecha (27 de Mayo de 2016)

3.2 Bytecoin (BCN)

Lanzada en Julio 4 de 2012, fue la primera moneda basa en CryptoNote, la implementación original de CryptoNote Java fue re-escrita usando C++. Bytecoin posee uno de los ecosistemas más grandes, y ha sido creada por el equipo de CryptoNote. Es la primera aplicación de ésta tecnología y hasta la fecha desarrolladores han estado haciendo contribuciones significativas al desarrollo de la tecnología CryptoNote.

3.2.3 Especificaciones

- Algoritmo usado: CryptoNight

- Tiempo por bloque: 120 segundos (2 Minutos)

- La dificultad reorientada por cada bloque

- Una moneda es divisible hasta 8 decimales (divisible 10^8 Unidades)

- Total de monedas: 18,446,744,073,709,551,616 unidades atómicas (= 184.46 billones de BCN).

- Tamaño máximo bloque (Maximum block size): En abril 11 de 2016, Bytecoin ha lanzado una nueva versión de ahí en adelante es capaz de utilizar transacciones de fusión y el tamaño de bloque se ha aumentado de 20,000 bytes a 100,000 bytes (0,1MB). [14]

- Promedio de tamaños de bloques: 3575 Bytes [15]

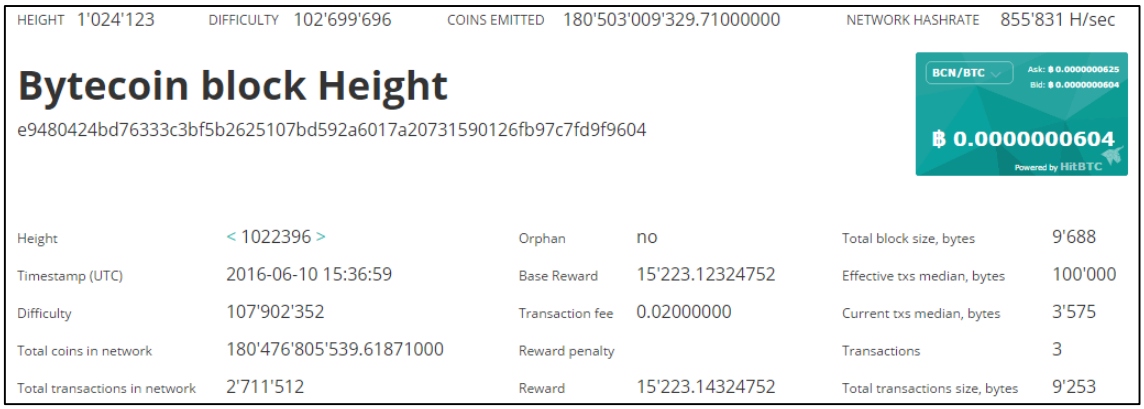


Ilustración 7. Block Heigh de Junio 2016 BYTECOIN [15]

- Transacciones por segundo: Máximo 12 TPS [16]

3.2.4 Información de la moneda

- Verdadera anonimidad y protección de datos
- Pagos in-rastreables usando firma digital
- Transacciones no detectables con datos aleatorios por el remitente
- Resistente al análisis de Blockchain (Cadena de bloques)
- Solo minado CPU & resistente a las ASIC
- Mecanismo POW en un sistema de voto para usuarios

Bytecoin Price	$0.000033 USD per BCN **	
Fecha Bloque Genesis	Wednesday, July 04, 2012 12:00:00 GMT	
Icono	Ⓑ	
Nombre	Bytecoin	
Simbolo / Etiqueta	BCN	
Website (Descarga Bytecoin Wallet)	https://bytecoin.org/	
Github / Código Fuente	Github https://github.com/amjuarez/bytecoin	
Foro	Bytecointalk https://bytecointalk.org/	
Bytecoin Wallet Version (Client Version)	v1.0.9.1 Get Info RPC Version: v1.0.9.1	Protocol Version: No info Wallet Version: No info
Status	Healthy	
Connections	8	
Algoritmo Hash	CryptoNight	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	18,446,744,073,709,551,616	
Tiempo generación bloque	2.00 minute(s)	
Recompensa por bloque	15,812.24502381 coins	
Block Count	1,012,442	
Bytecoin Difficulty	94799266	
Difficulty Retarget	1 blocks	

**** Bytecoin Price** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria BCN/BTC (27 de Mayo de 2016)

3.2.5 Algoritmo CryptoNight

Es un algoritmo creado por los desarrolladores de Bytecoin en cooperación con el equipo de CryptoNote [17] . Está diseñado para hacer que la CPU y la minería GPU sean más o menos igual de eficiente y restringir la minería ASIC[3].

CryptoNight es un algoritmo POW, diseñado para ser adecuado para las CPU de PC ordinarias, pero actualmente no hay dispositivos de propósito especial para la minería que están disponibles. Por lo tanto, CryptoNight sólo puede ser extraído-CPU por el momento.

CryptoNight se basa en el acceso aleatorio a la memoria lenta y hace hincapié en la dependencia de la latencia. Cada nuevo bloque depende de todos los bloques anteriores (a diferencia, por ejemplo, Scrypt). El algoritmo requiere alrededor de 2 MB por instancia:

1. Cabe en la memoria caché L3 (per core) de los procesadores modernos.

2. Un megabyte de memoria interna es casi inaceptable para los ASIC modernas.

3. Las GPU puede ejecutar cientos de instancias concurrentes, pero están limitados en otras formas. Memoria GDDR5 es más lento que el caché de la CPU L3 y notable por su ancho de banda, no por la velocidad de acceso aleatorio.

4. La expansión significativa de la memoria de trabajo necesitaría un aumento de iteraciones, que a su vez implica un incremento de tiempo global. Las llamadas “pesadas” en una red P2P de confianza, pueden conducir a serias vulnerabilidades, debido a que los nodos están obligados a chequear cada nuevo bloque POW.

Si el nodo gasta una cantidad considerable de tiempo en cada evaluación de hash, este puede ser fácilmente un ataque de denegación de servicios (DDoS) por un flujo de objetos falsos con los datos de trabajos arbitrarios (valores únicos).

3.2.6 CryptoNote

Dos de las principales características de cryptoNote son las firmas de anillo (Ring signatures) y las transacciones inconnectables (One-time keys: Unlinkable transactions). Las firmas de anillo ocultan la identidad del remitente mezclado y las transacciones inconectables crean las claves de un solo uso para los pagos individuales.

[3] ASIC es un circuito integrado para aplicaciones específicas, es un circuito integrado para un uso en particular, por ejemplo el chip diseñado solamente para la minería de Bitcoins.**Fuente especificada no válida.**

A Diferencia de bitcoin, los fondos no son guardados a la dirección que usted da a otros. En lugar de ello, cada vez que se reciba un pago que va a una dirección inconnectable generada con números aleatorios. Cuando usted decide gastar los fondos de esa dirección una sola vez, el importe se dividirá los componentes serán indistinguible de salidas idénticas en el blockchain. Cualquier cantidad arbitraria enviada en cualquier momento siempre se puede representar fundamentalmente **indistinguibles** (Una prueba matemática se da en CryptoNote v 2.0 [18] .

3.2.7 Las firmas de timbre

Ya se ha visto el concepto de firma, como se hace normalmente, entre A (alice) y B (bob). Donde solo hay un participante que permite el mapeo uno a uno:

Ilustración 8. Firma normal [19]

Una firma de timbre oculta la identidad porque solo prueba que el firmante pertenece a un grupo.

Ilustración 9. Firma de timbre [17]

Esto permite un alto nivel de anonimato en las transacciones de las criptomonedas.

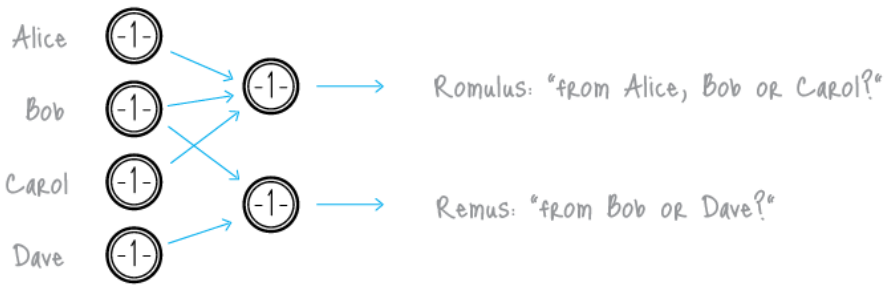


Ilustración 10. Transacciones irrastreables [19]

Cabe señalar que las transacciones extranjeras no te restringen el gasto de su propio dinero. La clave pública puede aparecer en el anillo de firmas de docenas de otros, pero sólo como un factor para salir del paso (Incluso si ya ha utilizado la clave secreta correspondiente para firmar su propia transacción). Por otra parte, si dos usuarios crean firmas de anillo con el mismo conjunto de claves públicas, las firmas serán diferentes (a menos que usen la misma clave privada).

3.2.8 Transacciones inconnectables

Normalmente, cuando publique su dirección pública, cualquier persona puede comprobar todas sus transacciones de entrada, incluso si están ocultos detrás de una firma de círculo. Para evitar la vinculación puede crear cientos de llaves y enviarlos a sus pagadores en privado, pero que priva de la conveniencia de tener una única dirección pública.

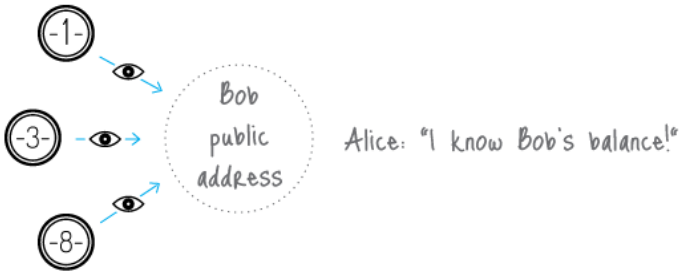


Ilustración 11. Transacciones inconnectables [19]

Perspectiva de una transacción [19] [20]:
Bob decide gastar una salida, la cual fue enviada a la clave pública única. Él necesita extra (1), TxOutNumber (2), y la clave privada de su cuenta (3) para recuperar la clave privada de un solo uso (4).

Cuando envía una transacción a Carol, Bob genera un valor Extra aleatoriamente (5). El usa Extra (6), TxOutNumber (7) y la clave pública de la cuenta de Carol (8) para conseguir su clave pública de salida (9).

En la entrada Bob oculta el enlace a su salida entre las claves externas (10). Para evitar doble gasto que también contiene la imagen clave, derivada de su clave privada de una sola vez (11).
Finalmente, Bob firma la transacción, usando su clave pública única (12), todas las claves publicas únicas (13) y la clave imagen (14). Se añade la Firma de timbre resultante hasta el final de la transacción (15).

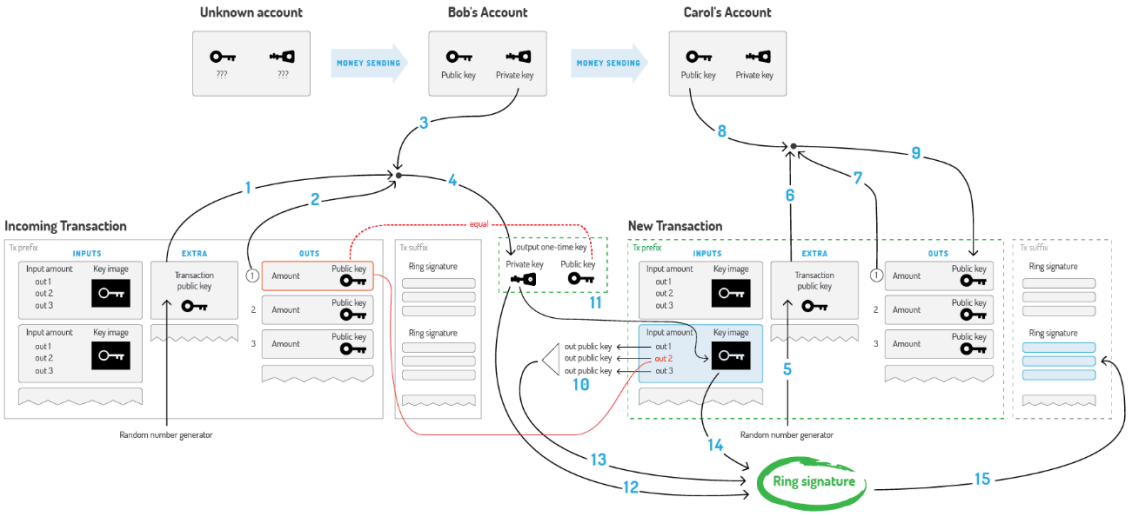


Ilustración 12. Transacción standard de CryptoNote [19]

3.3 Litecoin (LTC)

Alternativa al Bitcoin, fue lanzada en octubre 7 de 2011 por Charlie Lee, un empleado de Google, es una de las tres monedas con más capitalización después de Bitcoin y Ethereum. Es un proyecto Open-Source publicado bajo licencia MIT/X11 que otorga la posibilidad de ejecutar, modificar, copiar y distribuir el software a discreción, en copias modificadas del mismo. [21].

3.3.3 Especificaciones

- Algoritmo usado: Scrypt

- Tiempo por bloque: 2.50 minutos

- Recompensa por bloque: 25 coins a la fecha 27 de Mayo

- Bloque génesis: genex - {'date': 1317972665, 'magicbytes': 'fbc0b6db', 'name': 'Litecoin', 'starting_difficulty': 'fbc0b6db', 'merkle_root': '**97ddfbbae6be97fd6cdf3e7ca13232a3afff2353e29badfab7f73011edd4ced9**', 'port': 9333} (información obtenida de: https://minkiz.co/coin/136/ [22])

- Tamaño máximo bloque (Maximum block size): 1000000 Bytes = 1 MB [23]

- Promedio de tamaños de bloques: (Junio 2016) 8,303 bytes = 0.008303 MB [24]

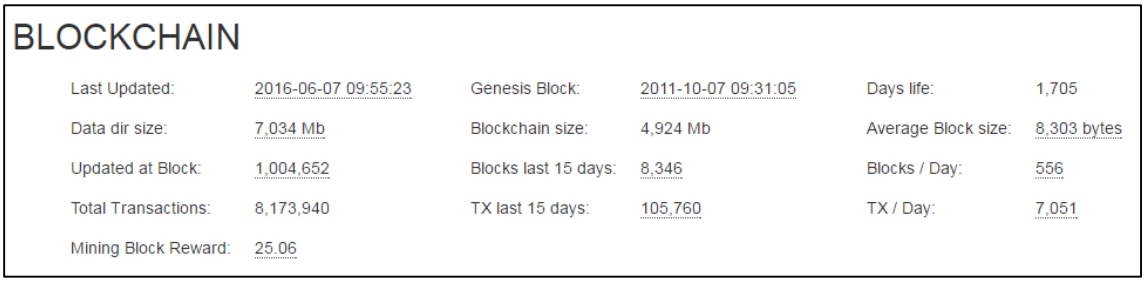


Ilustración 13. BlockChain Junio 2016 LITECOIN [24]

- Transacciones por segundo 4 veces más que bitcoin, es decir bitcoin actualmente está entre 3.3 tps y 7 tps, litecoin máximo 7*4 = 28 TPS [25]

3.3.4 Información de la moneda

Litecoin Price	$4.56 USD per LTC **	
Fecha Bloque Genesis	Saturday, October 08, 2011 06:29:19 GMT	
Icono		
Nombre	Litecoin	
Simbolo / Etiqueta	LTC	
Website (Descarga Litecoin Wallet)	https://litecoin.org/	
Github / Código Fuente	Github https://github.com/litecoin-project/litecoin	
Foro	Litecoin Forums https://litecointalk.org/	
Litecoin Wallet Version (Client Version)	v0.10.4.0-d1691e5 Get Info RPC Version: 100400	Protocol Version: 70003 Wallet Version: 60000
Status	Healthy	
Connections	8	
Algoritmo Hash	Scrypt	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	82,000,000	
Tiempo generación bloque	2.50 minute(s)	
Recompensa por bloque	25.00 coins	
Block Count	998,977	
Litecoin Difficulty	49646.8779	
Difficulty Retarget	2,016 blocks	

**** Litecoin Price** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria LTC/BTC (27 de Mayo de 2016)

3.4 Dogecoin (DOGE)

Fue creada por el programador Billy Markus y por Jackson Palmer Markus trabajador de marketing de Adobe, lanzada en Diciembre 8 de 2013 Ésta moneda es derivada de Litecoin, usa como símbolo un perro de raza Shiba Inu conocido en internet con el meme[4] de "Doge", es denominada como la moneda de internet divertida y amistosa, según la página oficial –dogecoin.com- una de las muchas monedas digitales que han sido lanzados después del éxito de Bitcoin. Dogecoin se presenta ampliamente basado en el protocolo Bitcoin,

[4] Meme de internet: Se usa para representar ideas, situaciones o expresiones de forma jocosa a través de imágenes, videos y otro tipo de multimedía.

pero con modificaciones. Utiliza la tecnología scrypt como un esquema de prueba de trabajo. Tiene un tiempo de bloque de 60 segundos (1 minuto) y el tiempo de dificultad reorientar es de cuatro horas. [26].

3.4.3 Especificaciones

- Algoritmo usado: Scrypt

- Tiempo por bloque: 1 Minuto

- La recompensa es de 10,000.00 coins por bloque a la fecha de 27 de Mayo de 2016.

- Bloque génesis: genex - {'date': 1386325540, 'magicbytes': 'c0c0c0c0', 'name': 'Dogecoin', 'starting_difficulty': 'c0c0c0c0', 'merkle_root': '**5b2a3f53f605d62c53e62932dac6925e3d74afa5a4b459745c36d42d0ed26a69**', 'port': 22556} (información obtenida de: https://minkiz.co/coin/61/ [27])

- Tamaño máximo bloque (Maximum block size): 1MB [28]

```
/** The maximum allowed size for a serialized block, in bytes (network rule) */
static const unsigned int MAX_BLOCK_SIZE = 1000000;
/** The maximum allowed number of signature check operations in a block (network rule)*/
static const unsigned int MAX_BLOCK_SIGOPS = MAX_BLOCK_SIZE/50;
```

- Promedio de tamaños de bloques: 7,371 bytes = 0.007371 MB [29]

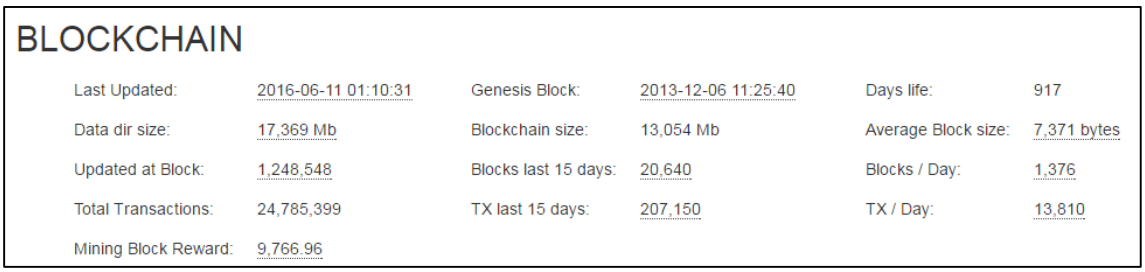


Ilustración 14. BlockChain Junio 2016 DOGECOIN [29]

3.4.4 Información de la moneda

Dogecoin Price	$0.000218 USD per DOGE **	
Fecha Bloque Genesis	Sunday, December 08, 2013 03:55:27 GMT	
Icono		
Nombre	Dogecoin	
Simbolo / Etiqueta	DOGE	
Website (Descarga Dogecoin Wallet)	http://dogecoin.com/	
Github / Código Fuente	Github https://github.com/dogecoin/dogecoin	
Foro	Bitcointalk https://bitcointalk.org/index.php?topic=361813.0	
Doge Wallet Version (Client Version)	v1.10.0.0-bb4b082 Get Info RPC Version: 1100000	Protocol Version: 70004 Wallet Version: 60000

Status	Healthy
Connections	8
Algoritmo Hash	Scrypt
Esquema Proof-of-Work	Proof-of-Work
Monedas disponibles	100,000,000,000
Tiempo generación bloque	1.00 minute(s)
Recompensa por bloque	10,000.00 coins
Block Count	1,229,219
Dogecoin Difficulty	19918.8469
Difficulty Retarget	1 blocks

** **Dogecoin** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria DOGE/BTC (27 de Mayo de 2016)

3.5 Verge (XVG)

Es un cambio de marca de DogeCoinDark, está creado para cumplir con los ideales originales de las criptomonedas, descentralizado y anónimo. Creado por ThomasV (original ltc fork) bitspill & sunerok (verge fork) [30]. Lanzada el 9 de octubre de 2014.

3.5.1 Especificaciones

- Algoritmo usado: Scrypt, x17, Lyra2rev2, myr-groestl, & blake2s [31]

- Tiempo de generación de bloque: ~5 minutos

- Plataformas Android, Linux, OSX, Windows, Web

- El número de monedas emitidas se ha fijado a 9 billones durante el primer año y un billon anuales a partir de entonces.

- Tamaño máximo bloque (Maximum block size): 1 MB [32]

```
31  static const int MULTI_ALGO_SWITCH_BLOCK = 340000;
32  static const unsigned int MAX_BLOCK_SIZE = 1000000;
```

- Promedio de tamaños de bloques: 378 bytes = 0.000378 MB [33]

BLOCKCHAIN

Last Updated:	2016-04-18 02:49:01	Genesis Block:	2014-10-09 20:22:44	Days life:	556
		Blockchain size:	240 Mb	Average Block size:	378 bytes
Updated at Block:	341,119	Blocks last 15 days:	21,184	Blocks / Day:	1,412
Total Transactions:	660,987	TX last 15 days:	22,130	TX / Day:	1,475

Ilustración 15. BlockChain Junio 2016 VERGE [33]

3.5.2 Información de la moneda

Verge Price	$0.000024 USD per XVG **	
Fecha Bloque Genesis	Thursday, October 09, 2014 19:04:47 GMT	
Icono		
Nombre	Verge	
Simbolo / Etiqueta	XVG	
Website (Descarga Verge Wallet)	http://vergecurrency.com/	
Github / Código Fuente	Github https://github.com/vergecurrency/VERGE	
Foro	Bitcointalk https://bitcointalk.org/index.php?topic=1365894	
Verge Wallet Version (Client Version)	v2.0.0.0-unk-beta Get Info RPC Version: v2.0.0.0-unk-beta	Protocol Version: 90001 Wallet Version: 60000
Status	Healthy	
Connections	12	
Algoritmo Hash	Scrypt	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	13,000,000,000	
Tiempo generación bloque	30.00 second(s)	
Recompensa por bloque	6,250.00 coins	
Block Count	425,158	
Verge Difficulty	67.8567	
Difficulty Retarget	1 blocks	

**** Verge Price** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria XVG/BTC (27 de Mayo de 2016)

3.6 Syscoin (SYS)

El proyecto utiliza funciones criptográficas del blockchain para crear aplicaciones que va a resolver los problemas del mundo real o entregar soluciones útiles, por ejemplo, verificar testamentos, fideicomisos , crear o construir plataformas de negociación de la comunidad. Se puso en marcha en abril de 2014, sin embargo la fecha del lanzamiento fue en Agosto 16 de 2014 por danosphere (usuario del foro bitcointalk) [34]

Por otro lado Syscoin recientemente (2016), fue re-lanzada denominándose así Syscoin 2.0, basada en Syscoin 1.0

3.6.1 Especificaciones

- Algoritmo usado: Scrypt

- Tiempo de generación de bloque: 60 segundos

- Syscoin ofrece servicios que permiten a los usuarios almacenar y recuperar posteriormente, los datos que se deseen directamente en la blockchain Syscoin. Hasta 256 KB de datos se puede almacenar por transacción. Sin embargo, un número arbitrario de operaciones SetData se puede realizar con el fin de almacenar la cantidad deseada de contenido en el blockchain Syscoin; el usuario sólo está limitado por la cantidad de cuotas que pueden permitirse el lujo de pagar. Los datos pueden ser recuperados posteriormente por el

almacenista o cualquier otra persona con el comando 'getData' de Syscoin junto con el ID de transacción de la transacción corresponsal 'SetData'. [35]

- Tamaño máximo bloque (Maximum block size): 2097152 bytes = 2.097152 MB [36]

```
28  /** The maximum allowed size for a serialized block, in bytes (network rule) */
29  static const unsigned int MAX_BLOCK_SIZE = (2 * 1024 * 1024);
```

- Promedio de tamaños de bloques: 738 Bytes = 0.000738 Mb [37]

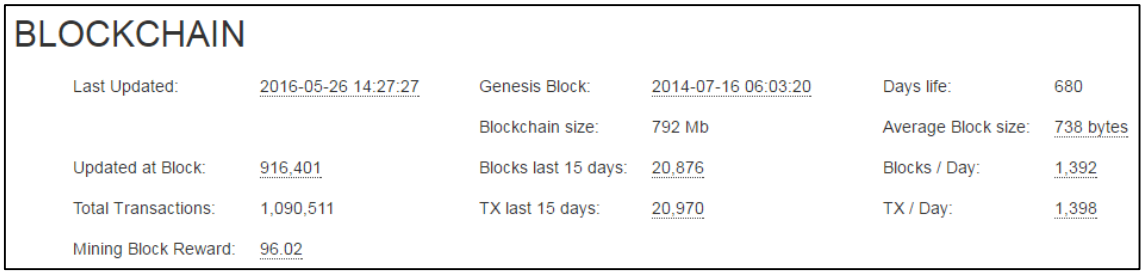


Ilustración 16. BlockChain Junio 2016 SYSCOIN [37]

3.6.2 Información de la moneda

Syscoin Price	$0.006758 USD per SYS **	
Fecha Bloque Genesis	Saturday, August 16, 2014 23:18:30 GMT	
Icono		
Nombre	Syscoin	
Simbolo / Etiqueta	SYS	
Website Descarga Syscoin wallet	http://syscoin.org/	
Github / Código Fuente	Github https://github.com/syscoin/syscoin	
Foro	Bitcointalk https://bitcointalk.org/index.php?topic=757255.0	
Syscoin Wallet Version Client Version	v0.8.6.4-g3b4bcea-beta Get Info RPC Version: 80604	Protocol Version: 70005 Wallet Version: 60000
Status	Unhealthy	
Connections	8	
Algoritmo Hash	Scrypt	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	2,000,000,000	
Tiempo generación bloque	1.00 minute(s)	
Recompensa por bloque	80.04659537 coins	
Block Count	897,171	
Bytecoin Difficulty	54.5917	
Difficulty Retarget	1 blocks	

**** Syscoin Price Price** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria SYS/BTC (27 de Mayo de 2016)

3.7 DigiByte (DGB)

Es una criptomoneda basa en Bitcoin y Litecoin, y más rápida que ellas, lanzada el 10 de junio de 2014 por Jared Tate, Digibyte es capaz de realizar 300 transacciones por segundo y es escalable para que coincida con la velocidad de transacciones de VISA para el año 2021.

3.7.1 Especificaciones

- Algoritmo Hashing: Scrypt

- Digibyte utiliza cinco algoritmos criptográficos muy avanzados (Grøstl "groestl", Qubit, scrypt, SHA-256 y Skein), estos cinco algoritmos de minería independiente procesan las transacciones a través de la red, proporciona tiempos de transacciones más rápidos con confirmaciones completas cada 1.5 minutos. Cada algoritmo representa aproximadamente el 20% de todos los bloques descubiertos en la red.

- Actualmente tres de los cinco algoritmos de Digibyte son resistentes ASIC y mucho mejor para los mineros GPU. Los mejores algoritmos GPU para minar son Groestl, Skein y Qubit. Es aun posible pero no es recomendado minar todos los cinco algoritmos con CPU. [38]

- Puede manejar 280+ transacciones por segundo.

- El proyecto planea suministrar un total de 21 billones de monedas a lo largo de 21 años. [39]

- La mineria de Digibyte es mucho más descentralizada, los algoritmos pueden ser cambiados en un futuro para prevenir la centralización.

- 1:1000 ratio. 1 Bitcoin for every 1000 DigiBytes

- Tamaño máximo bloque (Maximum block size): 8,388,608 bytes = 8 Mb [40]

- Promedio de tamaños de bloques: 250 Bytes = 0.00025 Mb a 585 Bytes = 0.000585 Mb [41]

BLOCKCHAIN

Last Updated:	2016-05-26 11:04:43	Genesis Block:	2014-01-10 22:13:14	Days life:	866
		Blockchain size:	1,993 Mb	Average Block size:	585 bytes
Updated at Block:	2,434,322	Blocks last 15 days:	86,629	Blocks / Day:	5,775
Total Transactions:	5,057,388	TX last 15 days:	132,877	TX / Day:	8,858
Mining Block Reward:	2,156.36				

Ilustración 17. BlockChain Junio 2016 DIGIBYTE [41]

- Transacciones por Segundo: 40 veces más rápido que Bitcoin, actualmente (año 2016) es 300 TPS, a su vez, estiman que para los próximos años tendrán capacidad de 200,000 TPS Para el 2035 [40]

3.7.2 Información de la moneda

DigiByte Price	$0.000304 USD per DGB **	
Fecha Bloque Genesis	Friday, January 10, 2014 22:27:56 GMT	
Icono		
Nombre	DigiByte	
Simbolo / Etiqueta	DGB	
Website (Descarga DigiByte Wallet)	http://www.digibyte.co/	
Github / Código Fuente	Github https://github.com/digibyte/DigiByteProject	
Foro	Bitcointalk	
DigiByte Wallet Version (Client Version)	v4.0.3.0-g354c0f3-DigiSpeed Get Info RPC	Version: 4000300 Protocol Version: 70003 Wallet Version: 60000
Status	Healthy	
Connections	8	
Algoritmo Hash	Scrypt	
Esquema Proof-of-Work	Proof-of-Work	
Monedas disponibles	21,000,000,000	
Tiempo generación bloque	15.00 second(s)	
Recompensa por bloque	1,019.64801735 coins	
Block Count	2,443,300	
DigiByte Difficulty	119.274	
Difficulty Retarget	144 blocks	

**** DigiByte Price** está basado en el precio más alto a la fecha y el más alto de la tasa cambiaria DGB/BTC (27 de Mayo de 2016)

4. Capítulo 4. Comparativa entre las monedas

4.1 Clasificación por algoritmos

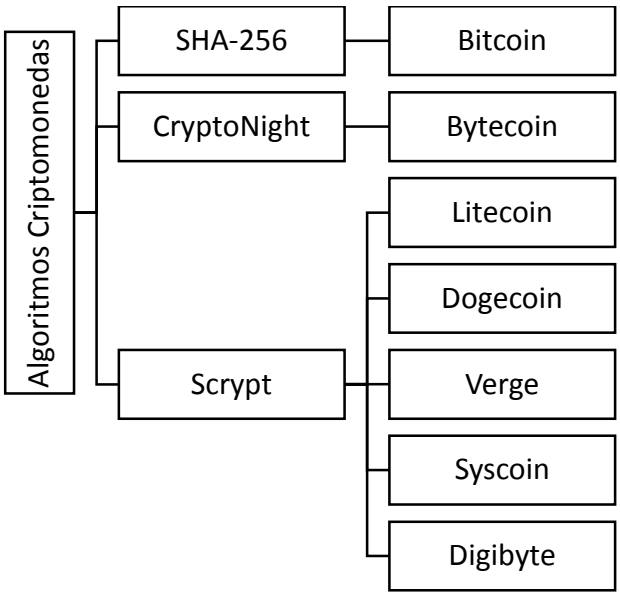


Ilustración 18. Clasificación de las monedas según su algoritmo

La moneda de Bitcoin, como se explicó en el 2. Capítulo 2 – Introducción a las criptomonedas, trabaja con el algoritmo SHA-256, mientras que la mayoría de las monedas como Litecoin, Dogecoin, Verge, Syscoin y Digibyte usan Scrypt, como idea principal el uso del algoritmo hash Scrypt era cambiar la forma de minar y los requerimientos de potencia de CPU. Las monedas basadas en Scrypt requieren menos potencia para ser generadas que las monedas SHA-256. Se debe tener en cuenta algo, en la historia de las monedas criptográficas se ha cambiado de CPU a GPU, y por último ASIC, el algoritmo Scrypt hace uso de los dispositivos ASIC, lo cual es una evolución del hardware para la minería de criptomonedas, lo cual se ha hecho muy competitivo su uso tanto para la minería de bitcoins como de las demás criptomonedas.

Litecoin fue la primera moneda en introducir el algoritmo de hash Scrypt, es el algoritmo de hash más común por altcoins, y el único otro algoritmo de hash para los que ahora existen dispositivos de hardware ASIC [35].

Las mejoras en el rendimiento de los ASIC en comparación con la minería CPU son más o menos similares para litecoin como para Bitcoin. En este sentido, litecoin falló en su objetivo original de crear un sistema más descentralizado mediante el mantenimiento de una comunidad de mineros de la CPU. Pero, más importante aún, esta narrativa todavía trabajaba para el arranque de litecoin, que atrajo muchos adoptantes que terminaron quedando incluso después de que la premisa original fracasara. Litecoin cambió la forma explícita de su principio, afirmando que su asignación inicial era más equitativa que Bitcoin del ASIC porque tenía cierta resistencia a los ASICs. [42]

La otra moneda que tiene un algoritmo particular es la Bytecoin, esta moneda tiene el algritmo CryptoNight que se describe en el apartado 3.2 Bytecoin (BCN) que a Diferencia de bitcoin, los fondos no son guardados a la dirección que se da a otros. En lugar de ello, cada vez que se reciba un pago que va a una dirección inconnectable generada con números aleatorios. En este caso la diferencia radica en la seguridad en que se realizan las transacciones.

4.2 Comparativas a nivel de bloques

La comparativa entre las monedas se han hecho teniendo en cuenta las propiedades de cada una como lo es: tamaño de transacciones por bloques, tiempo de generación entre un bloque y otro, tamaño máximo por bloque, se tomó en cuenta estas características para hacer los respectivos cálculos y compararlos con los que se han consultado y descrito en el apartado 3. Capítulo 3. Descripción de las criptomonedas, puesto que muchas referencias han cambiado en función del tiempo.

Los datos de la siguiente tabla se han tomado a partir de datos actuales al mes de Junio de 2016, de Coin of View [43] y de Chainradar para Bytecoin [15]. Por otro lado las fórmulas que se han usado para los cálculos son:

$$(Transacc.por\ Bloques) = \frac{Tamaño\ bloque\ (Max.Block\ Size)\ (Bytes)}{Prom.de\ tamaño\ de\ bloques\ generados\ (Bytes)}$$

$$(Transacc.por\ Segundo) = \frac{Tiempo\ de\ generacion\ bloques\ (MAX)}{Transacciones\ por\ bloques}$$

A continuación se presenta el cálculo de la moneda:

Moneda	Tamaño Bloque (Max. Block Size) (Bytes)	Tiempo de generación de bloques (Máximo) Segundos	Promedio de tamaño de bloques generados (Bytes)	Transacciones por bloques (Bytes)	Transacciones por segundo (TPS)
Bitcoin (min)	1000000	600	250	4000	7
Bitcoin (max)	1000000	600	500	2000	3,3
Bytecoin	1	120	3575	28,0	0,2
Litecoin	1000000	150	8303	120,4	0,8
Dogecoin	1000000	60	7371	135,7	2,3
Verge	1000000	30	378	2645,5	88,2
Syscoin	2	60	738	2841,7	47,4
DigiByte	8	15	585	14339,5	956,0

Tabla 1. Comparativa entre criptomonedas

Bitcoin (Min) Para calcular el TPS mínimo
Bitcoin (Max) Para calcular el TPS máximo

Al realizar los cálculos se ha notado que el TPS de algunas criptomonedas es demasiado bajo con respecto al TPS planteado por los desarrolladores. A continuación se hace un detalle de los cálculos planteados por los desarrolladores:

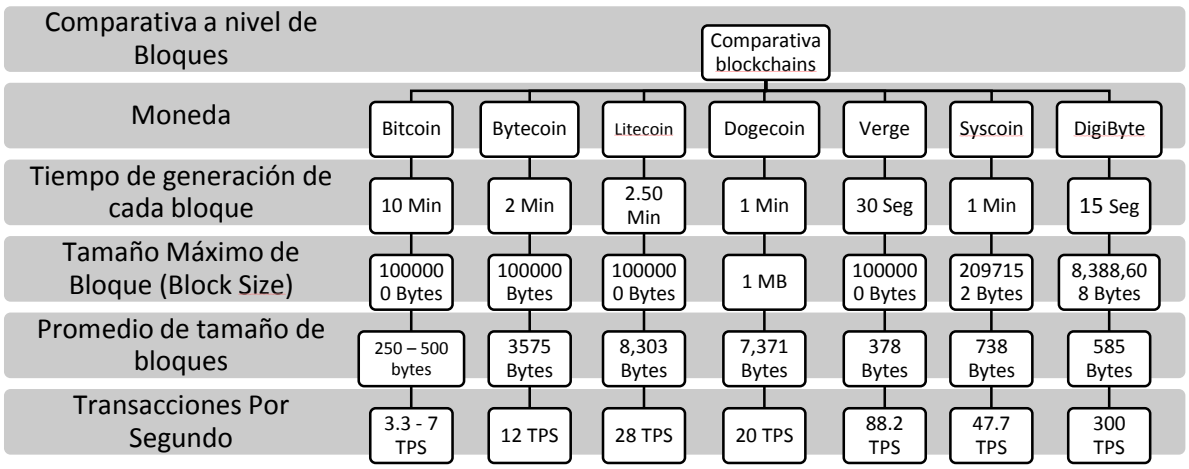


Tabla 2. Comparativa a nivel de Bloques

Analizando la tabla 1 y la tabla 2 hay discrepancia en los TPS mostrados excepto para la criptomoneda Bitcoin cuya información es más fácil de encontrar y calcular por el contrario Verge y Syscoin tienen el mismo TPS puesto que en la página de los desarrolladores no se ha encontrado información clara acerca de ello.
Por el contrario Bytecoin en los cálculos que se han hecho se ha encontrado un TPS bien bajo de 0.2 con respecto al planteado por los desarrolladores originalmente que es un máximo de 12 TPS y [16], teniendo en cuenta que en mayo de 2015 actualizaron, a 60 [44], quiere decir que no ha alcanzado a su máximo número de transacciones por segundo.

Igual que Bytecoin, la moneda Litecoin, según los creadores puede soportar 4 veces mayor su TPS con respecto al Bitcoin [25], es decir si bitcoin soporta 7 TPS , litecoin 28 TPS, sin embargo al hacer los cálculos el TPS fue menor 0.8 TPS.

Por otro lado tanto de Verge como de Syscoin no se tiene información acertada por parte de los desarrolladores y sus cálculos han sido tomando como referencias los que se han encontrado en la página.

Con la criptomoneda Digibyte, desde sus inicios ha sido ambicioso con las transacciones por segundo, según sus creadores es 40 veces más rápido que Bitcoin, actualmente (año 2016) el máximo es 300 TPS, a su vez, estiman que para los próximos años tendrán capacidad de 200,000 TPS Para el 2035 superando a VISA de 2000 [40]. Sin embargo, en los cálculos realizados el TPS calculado en la Tabla 1. Comparativa entre criptomonedas fue de 956, una cifra muy alta, que se puede pensar ha mejorado la capacidad de procesamiento, y van en miras de superar la que establecieron inicialmente.

Teniendo en cuenta la información anterior, se ha decidido trabajar con los datos calculados en la Tabla 1. Comparativa entre criptomonedas, puesto que estos datos son los más recientes y actuales, sin embargo algunas conclusiones están basadas en cuanto a desarrolladores y expertos en el tema que están en el día a día y en el minado de cada una de estas monedas.

Con respecto al Bitcoin, actualmente el límite de un bloque es de 1 MB, cualquier bloque por encima de 1MB es considerado invalido por la mayoría de los clientes BITCOIN, este límite corresponde a un máximo de aproximadamente 4000 transacciones por bloques (asumiendo que el tamaño promedio de transacciones sea entre 200 y 250 bytes, hasta febrero de 2016 [45] el tamaño varía entre 250 bytes y 500 bytes). Como los bloques son minados cada 10 minutos en promedio, esto da un maximum throughput de aproximadamente 7 transacciones por segundo. El tiempo de generación de cada bloque (blockchain) tarda 10 minutos o más para confirmar transacciones, se alcanzan 7 TPS máximo rendimiento (throughput). En comparación, un procesador de pagos corriente como tarjeta de crédito VISA confirma una transacción en cuestión de segundos, y procesa 2000 TPS, con una tasa máxima de 56000 TPS.

Si se compara el Bitcoin con las demás criptomonedas seleccionadas en relación con el TPS y las transacciones por bloques, se tiene que el TPS de Bitcoin se queda lejos con respecto a las transacciones por bloque máxima (4000 bytes) en relación con Digibyte que tiene un máximo TPS y una mayor transacción por bloques (14339.5 bytes), teniendo en cuenta que el tiempo promedio de generación por bloques es muy mínimo 15 Segundos. Por otro lado la criptomoneda Bytecoin presentó un número muy bajo de TPS, y las transacciones por bloques apenas si alcanzaron los 28 Bytes, teniendo así un promedio de bloque generado (3575 Bytes) muy superior al de Bitcoin (500 Bytes Max), se debe considerar que Bytecoin usa diferente algoritmo (CriptoNight) que puede influir en el tiempo de procesamiento, sin embargo ofreciendo más seguridad en las transacciones. Como se describe en el apartado 3.2.5 Algoritmo CryptoNight.

En un estudio reciente, el grupo de investigadores académicos del IC3 (Iniciativa por Criptodivisas y Contratos, en inglés: Initiative for CryptoCurrencies and Contracts) publicó un documento en donde se cuestiona la escalabilidad y propuestas actuales con respecto a la red bitcoin, con el fin de integrar un mayor número de usuarios sin riesgo a la saturación. [45]

El estudio ofrece contribuciones que permiten resolver el problema de escalabilidad. Con respecto al tamaño de los bloques, establece que no debe exceder los 4MB, dado el intervalo actual de 10 minutos entre bloques. Un máximo de 4MB corresponde a un rendimiento de 27 TPS. Proponen establecer un límite de latencia en el que el intervalo entre los bloques no sea menor de 12 Segundos, si se quiere alcanzar la utilización completa del ancho de banda en la red, esta contribución demarca los límites de la escalabilidad para así mantener la descentralización de la red.

Por otro lado, es necesario un rediseño del protocolo, de manera que la blockchain escale de manera significativa, sin afectar la descentralización, y concluyen que la reparametrización del límite de los bloques y su intervalo en la blockchain, son tan solo el primer paso hacia una mejora substancial de rendimiento y latencia, manteniendo la descentralización. [45] [13].

A continuación un resumen del total de monedas disponibles por cada criptomoneda:

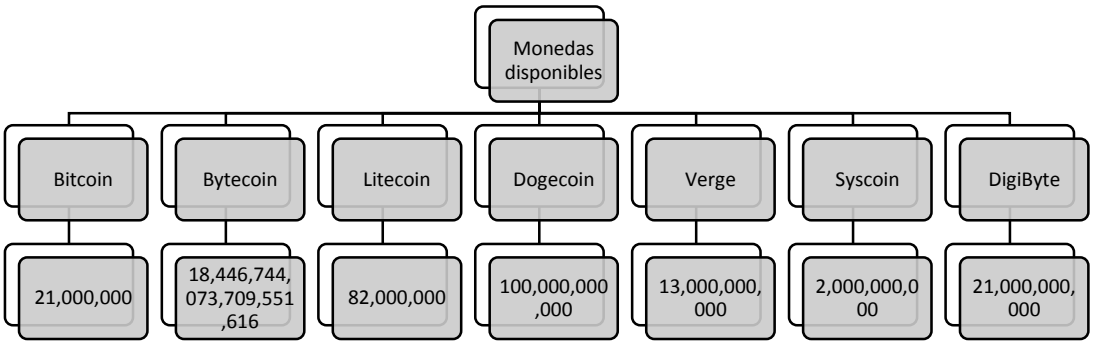


Ilustración 19. Total de monedas disponibles [a la fecha 2016]

5. Conclusiones

para comprender el funcionamiento de las criptomonedas y las propiedades de cada una de ellas, es necesario apropiarse de los conocimientos requeridos, puesto que cada moneda en cualquier momento puede decaer su valor otras pueden lograr un alto valor en el mercado como los es Bitcoin, que actualmente tiene una capitalización de más de 600 USD [46], sin embargo, se debe conocer qué hay detrás de éstas monedas, las alternativas que serán rentables en un futuro, el anterior trabajo se centró en describir las propiedades de cada una y tomando como referencia a la moneda Bitcoin se establecieron clasificaciones comparaciones entre ellas.

Durante la investigación se hizo el cambio de la moneda seleccionada al principio la moneda Earthcoin, la cual se cambió por Syscoin porque la moneda Earthcoin ha dejado de presentar transacciones visibles y no estaban muy claras.

Se encontró que la moneda Digibyte muy por encima de Bitcoin en cuanto a las transacciones por segundo, presenta un mayor número de transacciones por bloques y cuyo tiempo de generación es mucho menor a las demás monedas que se seleccionaron, esta moneda en particular llamó más la atención puesto que el tamaño máximo de bloques fue muy superior a las demás monedas seleccionada, recordando que según los desarrolladores Digibyte usa cinco algoritmos criptográficos muy avanzados (Grøstl “groestl”, Qubit, scrypt, SHA-256 y Skein), estos cinco algoritmos de minería independiente procesan las transacciones a través de la red, proporciona tiempos de transacciones más rápidos con confirmaciones completas cada 1.5 minutos. Cada algoritmo representa aproximadamente el 20% de todos los bloques descubiertos en la red. Se debe considerar también el tamaño máximo que tiene disponible cada moneda, esto podría influir en su capitalización y comercialización de la misma, la dificultad de minado puede aumentar o disminuir y los desarrolladores tendrán que buscar soluciones innovadoras.

Para finalizar, además de la cotización actual de la moneda, se debe tener en cuenta los cambios que puede surgir a futuro, conocer las propiedades y características de cada moneda, éste trabajo se centró en las monedas pow, sin embargo hay otras monedas que al igual que la líder (bitcoin) están compitiendo por ello como lo son las monedas con pruebas de participación (proof-of-stake).

6. Glosario

Altcoins: Criptomoneda que no es Bitcoin

Block Size: Tamaño de bloques (Bytes o Megabytes)

Block Time: Tiempo de bloque (En segundos o minutos)

Fusion Transactions: Transacciones de fusión, las operaciones de fusión proporcionan a os usuarios la posibilidad de optimizar automáticamente sus cuentas, el proceso de optimización se ejecuta en segundo plano, y es fácil de poner en marcha por la selección de una sola caja de configuración. Esta optimización es útil para aquellos usuarios cuyos Bytecoins están divididos en múltiples salidas pequeñas. Tal situación podría producirse si, por ejemplo, uno recibe un gran número de sugerencias a la cuenta o utiliza un pool, que transfiere dinero para el usuario en varios pagos pequeños (por ejemplo, las versiones anteriores de pool CryptoNote código abierto). Además de aumentar la comodidad, la optimización también mejorará el nivel de privacidad del propietario de la cartera. Técnicamente la optimización es una transacción de dinero libre de cargo para sí mismo de tal manera que el número de salidas (outputs) sea menos, mientras que los propios outputs se hacen más grandes. Tales transacciones se llaman Fusión de transacciones. Si el proceso de optimización está activado, la cartera seleccionará automáticamente las salidas que deben ser fusionados. [47]

Pool: Grupos que se dedican a minar, encontrar bloques denominadas también piscina de mineros, esto a cambio de recompensas divididas en cada uno de acuerdo al trabajo que han realizado.

Throughput: Rendimiento en el que blockchain puede confirmar transacciones.

Throughput máximo (Maximum throughput): El rendimiento máximo es la velocidad máximo a la que el block chain puede confirmar las transacciones. Ejemplo, en Bitcoin el rendimiento máximo es de 3.3 a 7 TPS, este número está limitado por el tamaño máximo de bloque y el tiempo inter-bloque (inter-block time)

7. Bibliografía

[1] CoinMarketCap, «Crypto-Currency Market Capitalizations,» 14 Marzo 2016. [En línea]. Available: http://coinmarketcap.com/currencies/views/all/.

[2] Bitcoin Project, «Bitcoin - Dinero P2P de código abierto,» 2016. [En línea]. Available: https://bitcoin.org/es/.

[3] Bitcoin P2P e-cash paper, «Bitcoin P2P e-cash paper,» 1 Noviembre 2008. [En línea]. Available: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.

[4] INCIBE, «Bitcoin: Una moneda Criptográfica,» 6 Febrero 2014. [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf.

[5] Bitcoin Wiki, «Bicoin Wiki FAQ,» 2016. [En línea]. Available: https://en.bitcoin.it/wiki/.

[6] Oro y Finanzas, «Oro y Finanzas,» 15 Enero 2016. [En línea]. Available: https://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm/.

[7] Oro y Finanzas, «Oro y Finanzas,» 15 Enero 2014. [En línea]. Available: https://www.oroyfinanzas.com/2014/01/criptografia-curva-eliptica-bitcoin-por-que-utiliza-ecdsa/. [Último acceso: Abril 2016].

[8] Bitcoin Wiki, «Proof of work,» 29 Enero 2016. [En línea]. Available: https://en.bitcoin.it/wiki/Proof_of_work. [Último acceso: Abril 2016].

[9] Blockchain.info, «Estadisticas Monetarias - Blockchain.info,» 16 Marzo 2016. [En línea]. Available: https://blockchain.info/stats.

[10] Bitcoin Wiki, «Bitcoin Wiki - Bloque,» 4 Octubre 2014. [En línea]. Available: https://es.bitcoin.it/wiki/Bloque.

[11] Coinwarz, «Cryptocurrencies,» 2016. [En línea]. Available: http://www.coinwarz.com/cryptocurrency/coins. [Último acceso: Mayo 2016].

[12] Coin of View, «Coin of View - Bitcoin,» [En línea]. Available: http://coinofview.com/coin/Bitcoin.html. [Último acceso: Junio 2016].

[13] Criptonoticias, «IC3 PUBLICA ESTUDIO DE PARÁMETROS PARA ESCALAR BITCOIN,» Abril 2016. [En línea]. Available: http://criptonoticias.com/ic3-publica-estudio-parametros-escalar-bitcoin/. [Último acceso: 2016 Junio].

[14] Bytecoin, «Bytecoin - New Block Size and RPC Wallet with Fusion Transactions,» [En línea]. Available: https://bytecoin.org/news/bytecoin-1.0.10-new-block-size-rpc-wallet-fusion-transactions/. [Último acceso: Junio 2016].

[15] Chainradar, «Chainradar - BYTECOIN,» Junio 2016. [En línea]. Available: http://chainradar.com/bcn/block/1022396. [Último acceso: Junio 2016].

[16] Bytecoin, «Future of Slacktivism. How 1,000,000 likes can save lives,» 16 Junio 2015. [En línea]. Available: https://bytecoin.org/blog/future-of-slacktivism/. [Último acceso: Junio 2016].

[17] CryptoNote, «CryptoNote - equal-proof-of-work,» Mayo 2016. [En línea]. Available: https://cryptonote.org/inside.php#equal-proof-of-work.

[18] CryptoNote, «CryptoNote v 2.0,» Mayo 2016. [En línea]. Available: https://cryptonote.org/whitepaper.pdf.

[19] Cryptonote, «Cryptonote Technology Inside,» [En línea]. Available: https://cryptonote.org/inside.php. [Último acceso: Mayo 2016].

[20] Bitcoin Forum, «Bitcoin Forum,» Mayo 2016. [En línea]. Available: https://bitcointalk.org/index.php?topic=622678.0.

[21] Wikipedia, «Litecoin,» 2016. [En línea]. Available: https://en.wikipedia.org/wiki/Litecoin. [Último acceso: Junio 2016].

[22] Minkiz, «Minkiz - Litecoin,» [En línea]. Available: https://minkiz.co/coin/136/. [Último acceso: Mayo 2016].

[23] Litecoin Wiki, «Litecoin Wiki - Transaction Fees,» [En línea]. Available: https://litecoin.info/Transaction_fees. [Último acceso: Mayo 2016].

[24] Coin of View, «Coin of View - Litecoin,» [En línea]. Available: http://coinofview.com/coin/Litecoin.html. [Último acceso: Junio 2016].

[25] Litecointalk Forum, «What's the deal with litecoins max transactions per second, and your thoughts?,» 2014. [En línea]. Available: https://archive.litecointalk.org/index.php?topic=23940.0. [Último acceso: 2016 Junio].

[26] Wikifix, «Dogecoin,» Diciembre 2014. [En línea]. Available: http://www.wikifx.info/sp/dogecoin/. [Último acceso: Mayo 2016].

[27] Minkiz, «Minkiz - Dogecoin,» [En línea]. Available: https://minkiz.co/coin/61/. [Último acceso: Junio 2016].

[28] Github, «Github - Dogecoin,» [En línea]. Available: https://github.com/dogecoin/dogecoin/search?utf8=%E2%9C%93&q=MAX_BLOCK_SIZE. [Último acceso: Junio 2016].

[29] Coin of View, «Coin of View - Dogecoin,» [En línea]. Available: http://coinofview.com/coin/Dogecoin.html. [Último acceso: Junio 2016].

[30] Github, «Vergecurrency / Electrum - XVG - Server,» [En línea]. Available: https://github.com/vergecurrency/electrum-xvg-server. [Último acceso: Junio 2016].

[31] Github, «Github - VERGE,» [En línea]. Available: https://github.com/vergecurrency/VERGE. [Último acceso: Junio 2016].

[32] Github, «Github - Verge,» [En línea]. Available: https://github.com/vergecurrency/VERGE/blob/87922b3d035d92340055996f0060a093d09a89b5/src/main.h. [Último acceso: Junio 2016].

[33] Coin of View, «Coin of View - Verge,» [En línea]. Available: http://coinofview.com/coin/Verge.html. [Último acceso: Junio 2016].

[34] Bitcoin Forum, «Bitcoin Forum - Syscoin,» [En línea]. Available: https://bitcointalk.org/index.php?topic=587080.0. [Último acceso: Junio 2016].

[35] Syscoin, «Syscoin Whitepaper,» [En línea]. Available: https://dl.dropboxusercontent.com/u/25508862/Syscoin/presale_ann/SyscoinWhitepaper-OverviewDraft.pdf. [Último acceso: Junio 2016].

[36] Github, «Github - Syscoin,» [En línea]. Available: https://github.com/syscoin/syscoin/search?utf8=%E2%9C%93&q=MAX_BLOCK_SIZE&type=Code. [Último acceso: Junio 2016].

[37] Coin of View, «Coin of View - Syscoin,» [En línea]. Available: http://coinofview.com/coin/Syscoin.html. [Último acceso: Junio 2016].

[38] Bitcoin Forum, «Bitcoin Forum - DigiByte [DGB],» [En línea]. Available: https://bitcointalk.org/index.php?topic=408268.0. [Último acceso: Junio 2016].

[39] Cryptocoin.cc, «Cryptocoin.cc - Digibyte,» [En línea]. Available: http://cryptocoin.cc/table.php?cryptocoin=digibyte. [Último acceso: Junio 2016].

[40] Digibyte, «How does DigiByte compare to Bitcoin?,» [En línea]. Available: http://www.digibyte.co/about. [Último acceso: Junio 2016].

[41] Coin of View, «Coin of view - Digibyte,» [En línea]. Available: http://coinofview.com/coin/DigiByte.html. [Último acceso: Junio 2016].

[42] A. Narayanan, J. Bonneau, E. Felten, A. Miller y S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Nueva Jersey: Princeton University Press, 2016, pp. 270 - 272.

[43] Coin of View, «Coin of View - All Coins,» [En línea]. Available: http://coinofview.com/all-coins.html. [Último acceso: Junio 2016].

[44] Bytecointalk, «Bytecointalk - Bytecoin 1.0.4 released,» [En línea]. Available: https://bytecointalk.org/showthread.php?tid=47. [Último acceso: Junio 2016].

[45] Initiative for CryptoCurrencies and Contracts IC3, «On Scaling Decentralized Blockchains - A Position Paper,» Febrero 2016. [En línea]. Available: http://www.initc3.org/scalingblockchain/full.pdf. [Último acceso: Junio 2016].

[46] Coinmarketcap, «Coinmarketcap - Crypto-Currency Market Capitalizations,» Junio 2016. [En línea]. Available: http://coinmarketcap.com/. [Último acceso: Junio 2016].

[47] CryptoNote Forum, «CryptoNote Forum - New Bytecoin Release 1.0.8 introduces fusion transactions,» [En línea]. Available: https://forum.cryptonote.org/viewtopic.php?f=12&t=732.

[48] Bitcoin Wiki, «Technical background of version 1 Bitcoin addresses,» 29 Enero 2016. [En línea]. Available: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses. [Último acceso: Abril 2016].

[49] Oro y Finanzas, «¿Cómo se crea una dirección o clave pública en Bitcoin? (X),» 21 Enero 2014. [En línea]. Available: https://www.oroyfinanzas.com/2014/01/como-crea-direccion-clave-publica-bitcoin/. [Último acceso: Abril 2016].

[50] CryptoNote, «CryptoNote - Inside,» [En línea]. Available: https://cryptonote.org/inside.php. [Último acceso: Mayo 2016].