Análisis y comparación de monedas criptográficas basadas en la tecnología blockchain

Máster Universitario En Seguridad De Las Tecnologías De La Información Y De Las Comunicaciones (Mistic)

Trabajo de Fin de Master

Autor: Maria Fernanda Medina Reyes

Consultor: Jordi Herrera Joancomartí

Junio de 2016

UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

Contenido

Descripción y presentación del proyecto

Bitcoin como referente

Criptomonedas

Clasificación

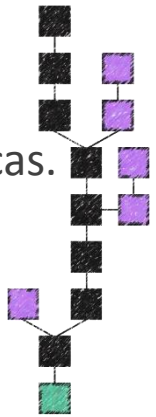
Conclusiones

Bibliografía

Descripción y presentación del proyecto

Objetivo General

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



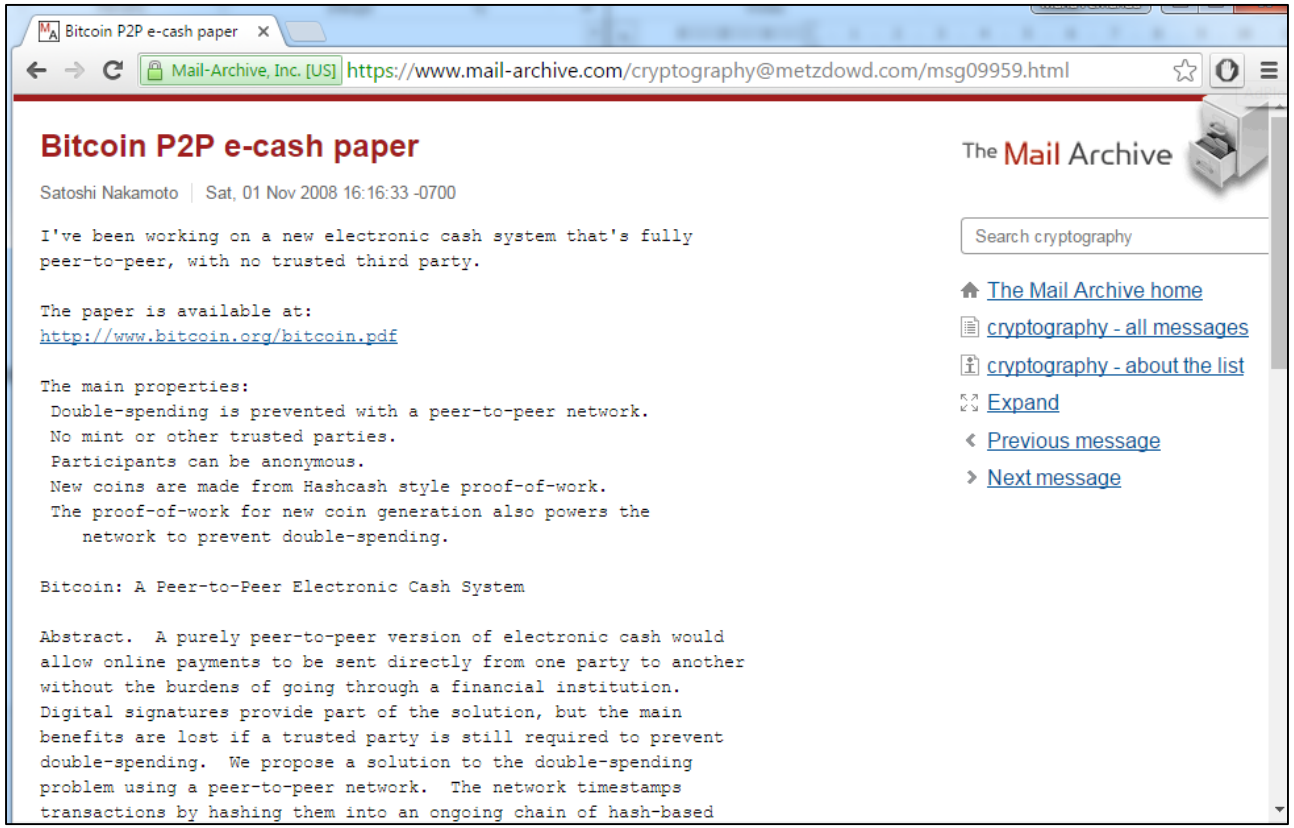
Objetivos Específicos

- ✓ Seleccionar las monedas criptográficas basadas en la tecnología *blockchain* 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

Bitcoin como referente…

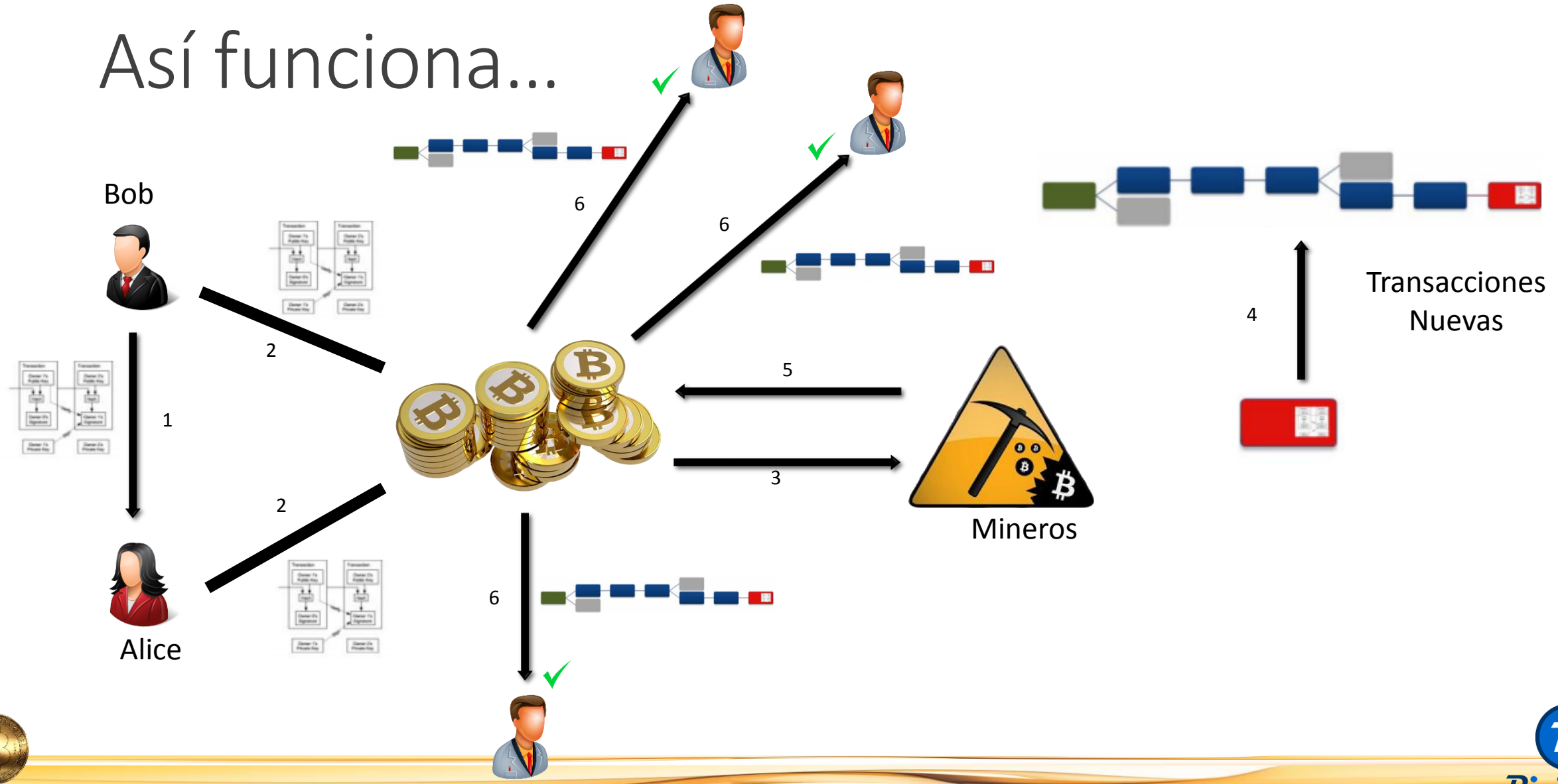
Moneda digital descentralizada

En 2008, Satoshi Nakamoto publicó en la lista de correo la primera especificación del protocolo de red de Bitcoin.



Mensaje de Satoshi Nakamoto en la lista de correos

Así funciona...



Detrás de la criptomoneda…

Funciones Hash

Firmas digitales

- SHA-256
- Curva elíptica ECDSA

Prueba de trabajo

Bloques

Cadena de bloques

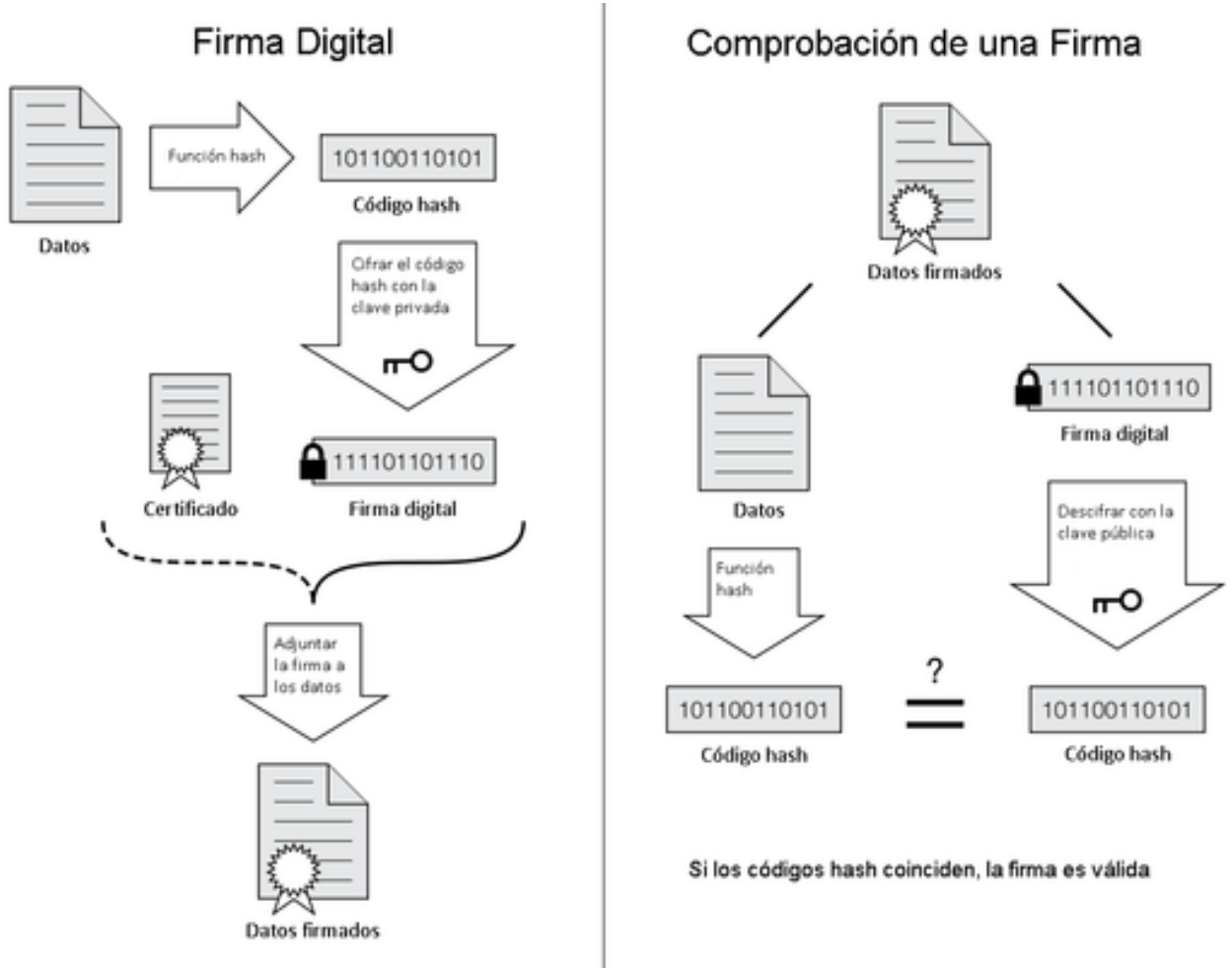
Clave pública

Transacciones por segundo (TPS)

Syscoin

Firmas digitales

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).



Proceso Firma digital

Detrás de la criptomoneda…

Funciones Hash

Firmas digitales

- SHA-256
- Curva elíptica ECDSA

Prueba de trabajo: Proof of work, en inglés, son el principal componente de Bitcoin responsable de garantizar que la red mantiene un comportamiento legítimo.

Bloques

Cadena de bloques

Bloques

Los campos de un bloque son:

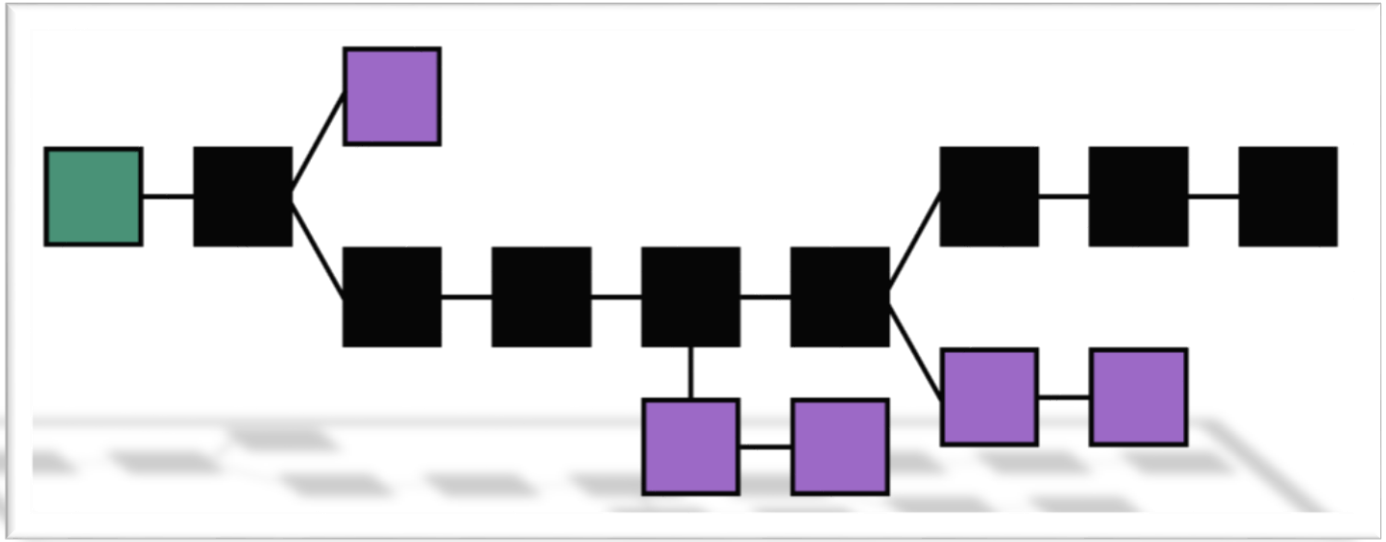
- Magic no
- Blocksize
- Blockheader
- Transaction counter
- Transactions

La cabecera del bloque contiene:

Version
HashPrevBlock
HashMerkletRoot
Time
Bits
Nonce

Cadena de bloques

Cadena de bloques o *Blockchain* en inglés, 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.



Clave pública

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

Syscoin

Transacciones por segundo (TPS)

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

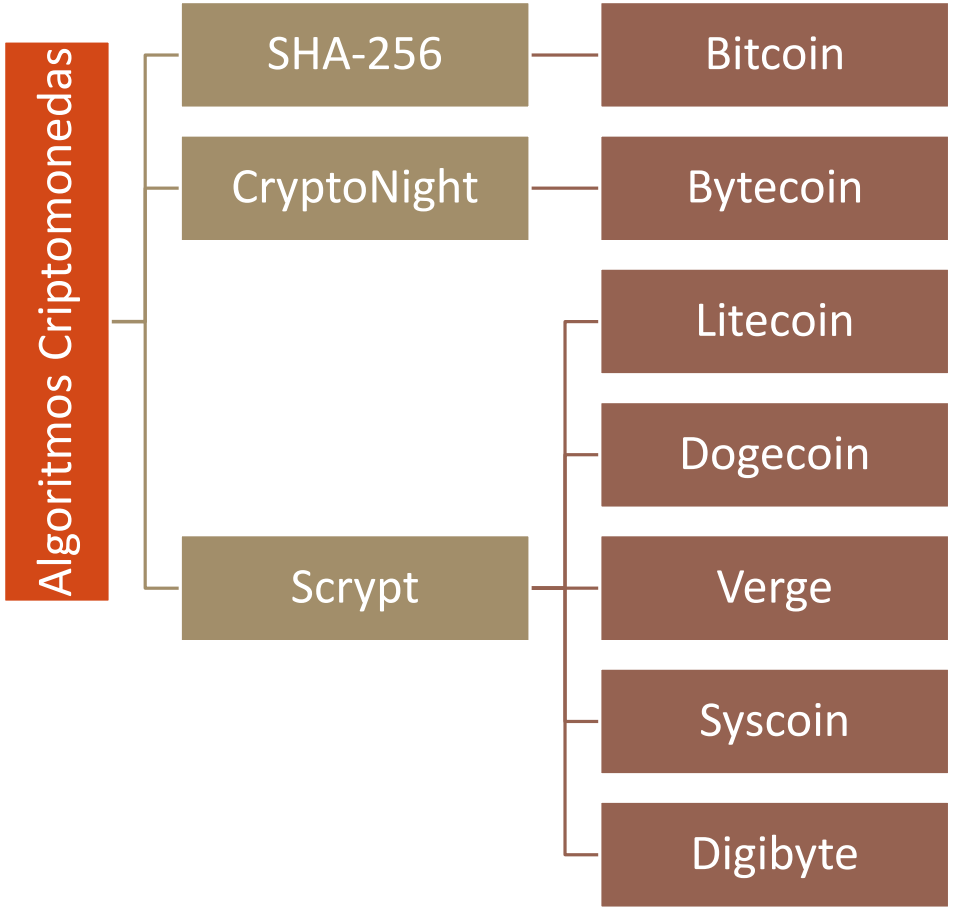
Ejemplo:

$$\frac{1{,}000{,}000\ bytes}{257\ bytes\ * 600\ segs} = 6.8\ TPS$$

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).

Clasificación | Algoritmos



Clasificación en cuanto a propiedades

- ✓Tamaño Bloque (Max. Block Size)
- ✓Tiempo de generación de bloques, en segundos
- ✓Promedio de tamaño de bloques en Bytes
- ✓Transacciones por bloques en Bytes
- ✓Transacciones por segundo (TPS)

Syscoin

Clasificación en cuanto a propiedades

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

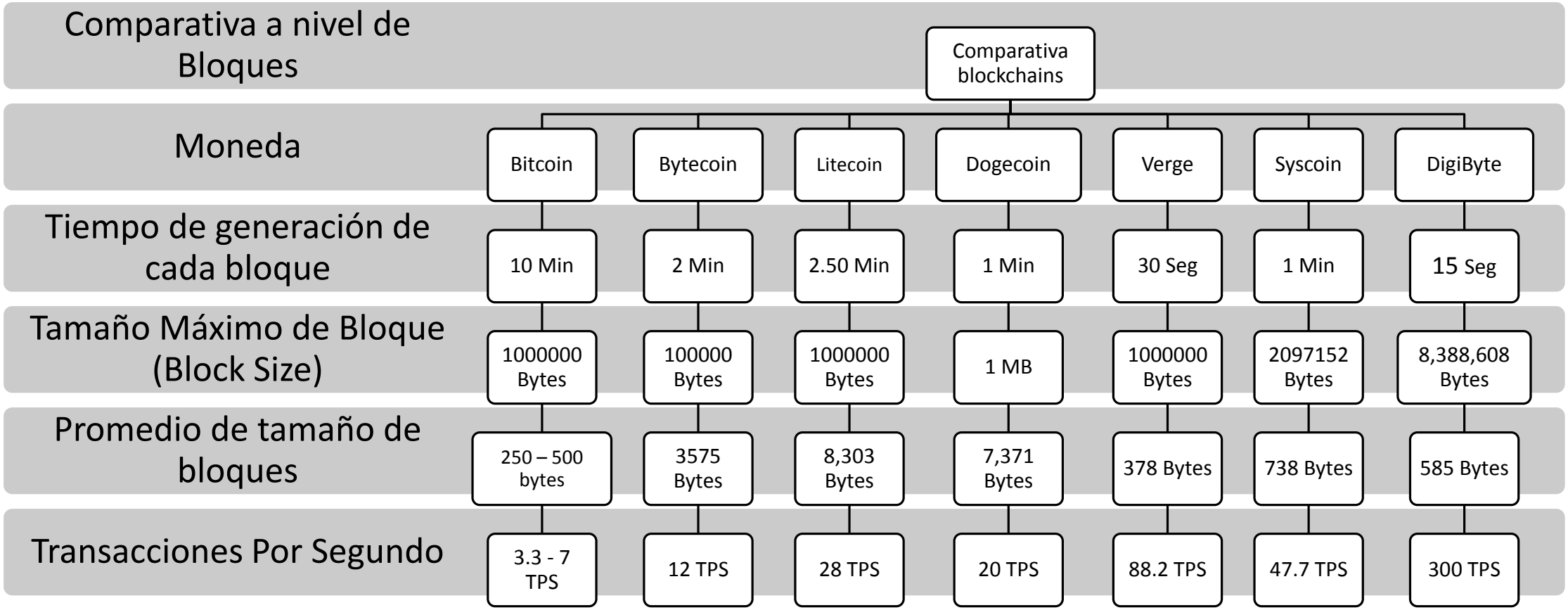
$$(Transacc.por\ Bloques) = \frac{Tamaño\ bloque\ (Max.Block\ Size)\ (Bytes)}{Prom.de\ tamaño\ de\ bloques\ generados\ (Bytes)}$$

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

Resultado de los cálculos…

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 (max)	1000000	600	500	2000	3,3
Bitcoin (min)	1000000	600	250	4000	7
Bytecoin	100000	120	3575	28,0	0,2
DigiByte	8388608	15	585	14339,5	956,0
Dogecoin	1000000	60	7371	135,7	2,3
Litecoin	1000000	150	8303	120,4	0,8
Syscoin	2097152	60	738	2841,7	47,4
Verge	1000000	30	378	2645,5	88,2

Clasificación en cuanto a propiedades



Conclusiones

- ✓Para conocer alternativas que serán rentables en un futuro es necesario apropiarse de los conocimientos requeridos, el funcionamiento y las propiedades de cada una de ellas.

- ✓No todas las altcoins se mantienen con el tiempo, se hizo cambio de una moneda puesto que sus especificaciones y transacciones no estaban muy claras y pocos visibles.

- ✓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

Conclusiones

- ✓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).

Bibliografía

- ✓CoinMarketCap, «Crypto-Currency Market Capitalizations,» 14 Marzo 2016. [En línea]. Available: http://coinmarketcap.com/currencies/views/all/.
- ✓INCIBE, «Bitcoin: Una moneda Criptográfica,» 6 Febrero 2014. [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/int_bitcoin.pdf
- ✓Bitcoin Wiki, «Bicoin Wiki FAQ,» 2016. [En línea]. Available: https://en.bitcoin.it/wiki/
- ✓Blockchain.info, «Estadisticas Monetarias - Blockchain.info,» 16 Marzo 2016. [En línea]. Available: https://blockchain.info/stats
- ✓Coinwarz, «Cryptocurrencies,» 2016. [En línea]. Available: http://www.coinwarz.com/cryptocurrency/coins. [Último acceso: Mayo 2016]
- ✓Bitcoin Forum, «Bitcoin Forum,» Mayo 2016. [En línea]. Available: https://bitcointalk.org/index.php?topic=622678.0