Acostumbrados a correcciones del 30% que duraban unos pocos días o semanas, estos tres meses que llevamos de mercado bajista están acabando con la paciencia de más de uno. Las noticias vuelven a ser bastante pesimistas, donde muchos dan por hecho la explosión de la burbuja de bitcoin (una vez más), pero si leemos maravillas de la tecnología blockchain.

Esto como sabéis no tiene sentido en nuestra opinión. Cada vez que escuchéis a alguien hablar bien de blockchain pero no gustarle Bitcoin o Ethereum, podéis salir corriendo porque esa persona tiene poca idea de lo que significan estas redes descentralizadas. Blockchain no tiene ningún sentido sin el efecto red y la base monetaria que produce la existencia de monedas como bitcoin o ether. Es decir, parte de la tecnología blockchain es el incentivo económico para utilizar y mantener estas redes: su moneda.

Hablar bien de blockchain y mal de las principales criptodivisas es como hablar bien de los coches pero hablar mal de la gasolina. ¿Es posible que en un futuro veamos coches que funcionan con agua o electricidad? Seguro que sí, pero de momento el combustible que manda es el petróleo.

En nuestro ejemplo, las gasolinas más demandadas actualmente en el ecosistema blockchain se llaman bitcoin y ether, y por tanto la mayor parte de servicios y ecosistema alrededor de blockchain integran y aceptan estos dos tipos de “gasolina”.

¿Estos tipos de criptomonedas pueden cambiar y evolucionar? Por supuesto que sí, bitcoin y ether de momento son dos experimentos que empiezan a tener un uso real y una adopción, pero todavía es bajísima en comparación con nuestro ejemplo de la

gasolina. Aun así ambos experimentos son los que tienen mayor potencial de supervivencia, y si lo consiguen, sus rentabilidades serán estratosféricas.

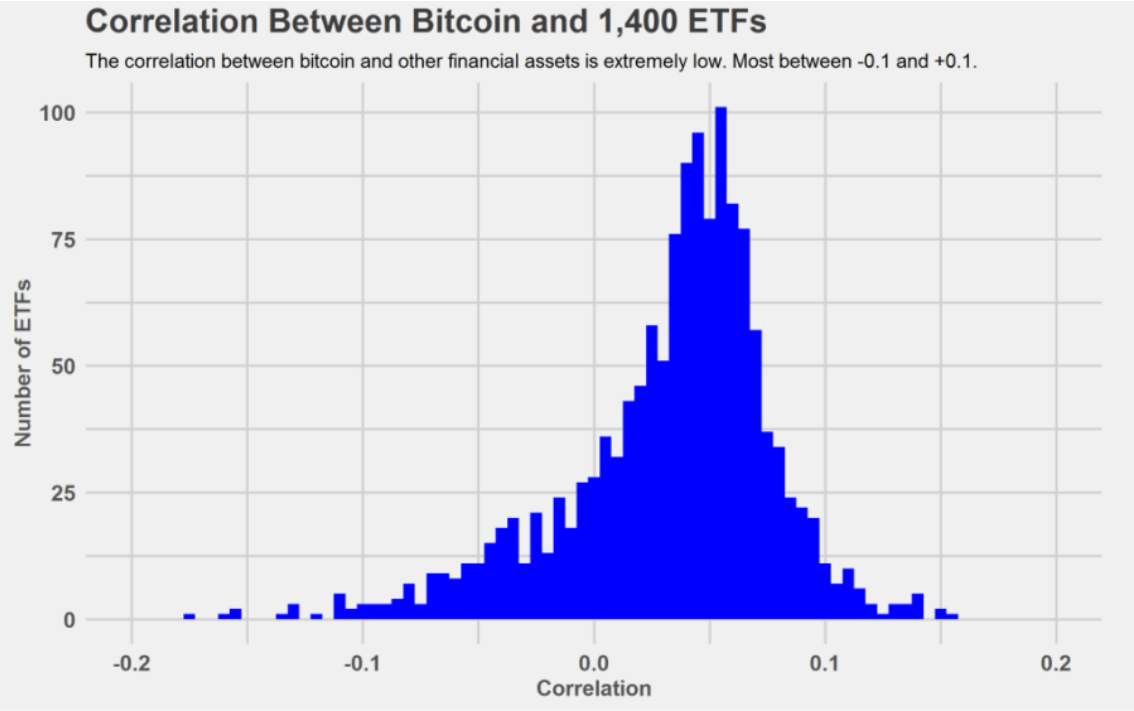
Entendemos el desánimo que puede provocar un mercado bajista de meses e incluso años. Lo notamos hasta en nuestros suscriptores, ya que un mes más nos encontramos sin ningún tipo de pregunta. Nosotros vivimos de cerca otra burbuja de bitcoin en 2014, la cual desencadenó un mercado bajista de año y medio:

Si miramos este mercado bajista con perspectiva, vemos que tan sólo supuso una espectacular oportunidad de compra:

¿Estamos ante un mercado bajista de meses incluso años parecido al que tuvimos en 2014? Creemos que no, ya que en su día el desconocimiento de Bitcoin era total a todos los niveles. Bitcoin por aquel entonces era un motivo de mofa o burla en muchos foros, y aunque seguimos viendo mucho escepticismo, también ha aumentado

considerablemente la seriedad con la que algunas empresas e instituciones tratan a estas redes descentralizadas.

Además, la capitalización del mercado y el volumen de negociación ahora se sitúa en unos niveles asumibles por un inversor institucional, y la descorrelación que ofrece este nuevo tipo de activo sin duda hace que muchos fondos se planteen seriamente el incluirlo como un nuevo tipo de activo dentro de sus estrategias:

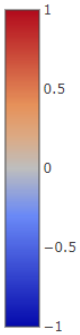


Este gráfico es muy interesante, ya que se han elegido los 1400 ETF con mayor volumen de distintos tipos de activo y se ha calculado la correlación histórica con bitcoin. La solución es que todos los activos tradicionales correlacionan entre -0.2 y 0.2 con bitcoin, y por tanto su comportamiento es totalmente distinto.

Sin embargo, también hay que comentar el aumento de correlación entre las propias criptomonedas, ya que al ser un mercado cada vez más maduro, en momentos de pánico tendemos a ver correlaciones altas entre los distintos activos digitales:

Cryptocurrency Correlation Matrix, 90-Days

	BTC	ETH	XRP	BCH	LTC	XLM	XEM	XMR	DASH	ETC	LSK	ZEC	SC	REP	FCT	NXT	^SPX	^VIX	^GLD	^TNX
BTC	1	0.81	0.5	0.65	0.86	0.62	0.66	0.85	0.83	0.73	0.72	0.75	0.67	0.61	0.76	0.52	0.12	-0.24	0.05	0.04
ETH	0.81	1	0.54	0.7	0.79	0.65	0.76	0.82	0.83	0.85	0.74	0.8	0.64	0.74	0.79	0.5	0.21	-0.32	0.15	0.15
XRP	0.5	0.54	1	0.32	0.47	0.76	0.65	0.48	0.51	0.5	0.54	0.49	0.55	0.37	0.51	0.28	0.18	-0.23	0.18	-0.08
BCH	0.65	0.7	0.32	1	0.65	0.41	0.56	0.8	0.84	0.66	0.64	0.78	0.61	0.67	0.65	0.51	0.02	-0.22	0.09	0.13
LTC	0.86	0.79	0.47	0.65	1	0.61	0.65	0.78	0.82	0.75	0.72	0.74	0.67	0.62	0.73	0.59	0.23	-0.32	0.14	0.13
XLM	0.62	0.65	0.76	0.41	0.61	1	0.72	0.59	0.64	0.6	0.57	0.62	0.6	0.45	0.7	0.4	0.22	-0.26	0.19	-0.03
XEM	0.66	0.76	0.65	0.56	0.65	0.72	1	0.66	0.71	0.66	0.65	0.65	0.69	0.62	0.74	0.53	0.18	-0.28	0.09	0.04
XMR	0.85	0.82	0.48	0.8	0.78	0.59	0.66	1	0.9	0.72	0.73	0.87	0.7	0.69	0.81	0.57	0.08	-0.25	0.05	0.16
DASH	0.83	0.83	0.51	0.84	0.82	0.64	0.71	0.9	1	0.76	0.78	0.87	0.79	0.7	0.8	0.59	0.13	-0.28	0.09	0.15
ETC	0.73	0.85	0.5	0.66	0.75	0.6	0.66	0.72	0.76	1	0.67	0.77	0.54	0.64	0.76	0.47	0.18	-0.3	0.12	0.09
LSK	0.72	0.74	0.54	0.64	0.72	0.57	0.65	0.73	0.78	0.67	1	0.76	0.71	0.59	0.73	0.59	0.1	-0.22	0.14	0.08
ZEC	0.75	0.8	0.49	0.78	0.74	0.62	0.65	0.87	0.87	0.77	0.76	1	0.72	0.68	0.81	0.55	0.08	-0.23	0.05	0.1
SC	0.67	0.64	0.55	0.61	0.67	0.6	0.69	0.7	0.79	0.54	0.71	0.72	1	0.49	0.68	0.57	0.19	-0.23	0.12	0.03
REP	0.61	0.74	0.37	0.67	0.62	0.45	0.62	0.69	0.7	0.64	0.59	0.68	0.49	1	0.64	0.44	0.06	-0.12	0.13	0.24
FCT	0.76	0.79	0.51	0.65	0.73	0.7	0.74	0.81	0.8	0.76	0.73	0.81	0.68	0.64	1	0.54	0.11	-0.23	0.06	-0.01
NXT	0.52	0.5	0.28	0.51	0.59	0.4	0.53	0.57	0.59	0.47	0.59	0.55	0.57	0.44	0.54	1	0.17	-0.2	0	0.11
^SPX	0.12	0.21	0.18	0.02	0.23	0.22	0.18	0.08	0.13	0.18	0.1	0.08	0.19	0.06	0.11	0.17	1	-0.82	0.21	0.09
^VIX	-0.24	-0.32	-0.23	-0.22	-0.32	-0.26	-0.28	-0.25	-0.28	-0.3	-0.22	-0.23	-0.23	-0.12	-0.23	-0.2	-0.82	1	-0.2	-0.17
^GLD	0.05	0.15	0.18	0.09	0.14	0.19	0.09	0.05	0.09	0.12	0.14	0.05	0.12	0.13	0.06	0	0.21	-0.2	1	-0.02
^TNX	0.04	0.15	-0.08	0.13	0.13	-0.03	0.04	0.16	0.15	0.09	0.08	0.1	0.03	0.24	-0.01	0.11	0.09	-0.17	-0.02	1



Aun así, por mucho que algunos intenten ver relaciones entre bitcoin y activos como la renta variable americana, el oro y los bonos de gobierno, la realidad es que la correlación es prácticamente despreciable.

En este estupendo enlace https://www.sifrdata.com/ encontraréis herramientas para poder visualizar estas correlaciones y cómo han ido cambiando a lo largo del tiempo (correlaciones rolling). Pero la principal idea que queremos transmitir con todo esto es que al margen del potencial socio-económico que tienen los activos digitales, como instrumento de inversión la descorrelación que ofrecen suponen un atractivo para determinados fondos de inversión.

La buena noticia es que la mayor parte de estos fondos de inversión todavía no tienen activos digitales en cartera, ya que la custodia de este nuevo tipo de activo genera problemas, y los reguladores todavía no saben cómo tratarlo. Esto hace que por el inversor minorista (persona física) pueda acceder más fácilmente a este mercado que determinadas instituciones.

Desde Consultora Bitcoin pensamos que con la inclusión de nuevos instrumentos para el inversor institucional como ETF o futuros, el aluvión de entrada de capital institucional a estos activos digitales puede ser masivo, lo cual debería poner la capitalización del mercado de activos digitales muy por encima de los niveles actuales.

Por ello consideramos que en momentos de caídas y extremo pesimismo son la mejor oportunidad para estudiar y discernir los proyectos y protocolos que realmente tienen calidad y mayor probabilidad de quedarse con nosotros un largo periodo de tiempo.

DPOS - ¿Solución al problema de escalabilidad?

Antes de nada, quiero agradecer a Myles Snider, Kyle Samani, y Tushar Jain sus estupendas contribuciones en Medium (https://medium.com/) y otros canales, las cuales nos han ayudado a comprender mejor cuáles son las diferencias que ofrece DPOS (delegated proof of stake) en relación a los conocidos POW (proof of work) y POS (proof of stake).

POW es el principal algoritmo, implementado en Bitcoin y otras criptomonedas, y que soluciona a la perfección el llamado "problema de los generales bizantinos" (https://es.wikipedia.org/wiki/Problema_de_los_generales_bizantinos). El problema se centra en cómo generar consenso en una red descentralizada donde no te puedes fiar de nadie. Gracias a la prueba de trabajo que se establece en el algoritmo de Bitcoin, este problema es solucionado y podemos decir que **Bitcoin es la red descentralizada consensuada y no permisionada más segura del mundo**.

Sin embargo, esta prueba de trabajo que garantiza el consenso y la descentralización a su máximo exponente, también se consigue a costa de mermar otras variables que para determinados nichos de mercado pueden ser no menos importantes, como la velocidad de transmisión o el número de validadores de bloques.

No me malinterpretéis, el objetivo de esta sección es ayudar a comprender qué es DPOS y qué ventajas e inconvenientes ofrece sobre los conocidos POW de bitcoin y el POS ("proof of stake") al que quiere llegar Ethereum y que está implementado en otras redes.

Volviendo a la escalabilidad, encontramos variables importantes a tener en cuenta, algunas de las cuales DPOS consigue mejorar considerablemente, a costa de empeorar otras:

1. **Número de nodos involucrados en la generación/validación de bloques**. A medida que este número aumenta, podemos decir que estamos ante una red con mayor descentralización.

2. **Número de transacciones por segundo** que soporta la red, es una de las variables que mejora notablemente el algoritmo de DPOS.

3. **Seguridad de la red**: ¿cuánto me costaría un ataque bizantino que consiga engañar a la red para modificar alguna de las transacciones de sus bloques? La respuesta en caso de Bitcoin es incalculable: el coste es tan alto que podemos decir que Bitcoin es resistente a todo tipo de ataque bizantino y por tanto 100% consensuada. Sin embargo, ¿y si nuestro algoritmo consiguiera que el coste de este tipo de ataques fuera lo suficientemente alto y complicado

para que mereciera la pena el aumento en la velocidad y escalabilidad de la red?

4. **Latencia**: ¿el sistema me garantiza que la transacción llegará a su destino en un tiempo determinado? De ser así, ¿cuánto tengo que esperar? De no estar garantizado, ¿cómo evita el sistema un doble gasto si ya he enviado la transacción?

DPOS es un sistema que concentra la generación/validación de bloques en unos pocos agentes dándoles una especie de "confianza" en forma de voto, con el objetivo de alcanzar un número de transacciones por segundo muy superior a redes que trabajan con POW o POS.

El algoritmo que hay detrás de DPOS es creado por Dan Larimer en 2013 como base para su primer proyecto BitShares. Con el tiempo, perfecciona el algoritmo y lo utiliza en la creación de su segundo proyecto, una red descentralizada de generación y curación de contenido que ya conocemos en Consultora Bitcoin: STEEM. Para los nuevos suscriptores, recomiendo leer el informe de Agosto 2017, dedicado a esta criptomoneda.

Actualmente tenemos varios proyectos que están utilizando este algoritmo de consenso: EOS, STEEM, BitShares, Lisk, PeerPlays, Nano, etc.

En DPOS, los tenedores de moneda tienen el poder para elegir mediante votación a los que producen y validan los bloques, y su voto será proporcional a la cantidad de moneda que tengan. Esto convierte el DPOS en una especie de democracia representativa y líquida de una red descentralizada, cuyo sufragio está representado por los que tienen interés en la plataforma: los tenedores de la criptomoneda.

Esto hace que en DPOS, a diferencia de otros modelos, tengamos una gobernanza establecida en el código, la cual dará una respuesta rápida, transparente y democrática en posibles eventos de desacuerdo o incluso fork, como los que hemos vivido en Bitcoin (Bitcoin Cash) y en Ethereum (ETH vs Ethereum Classic).

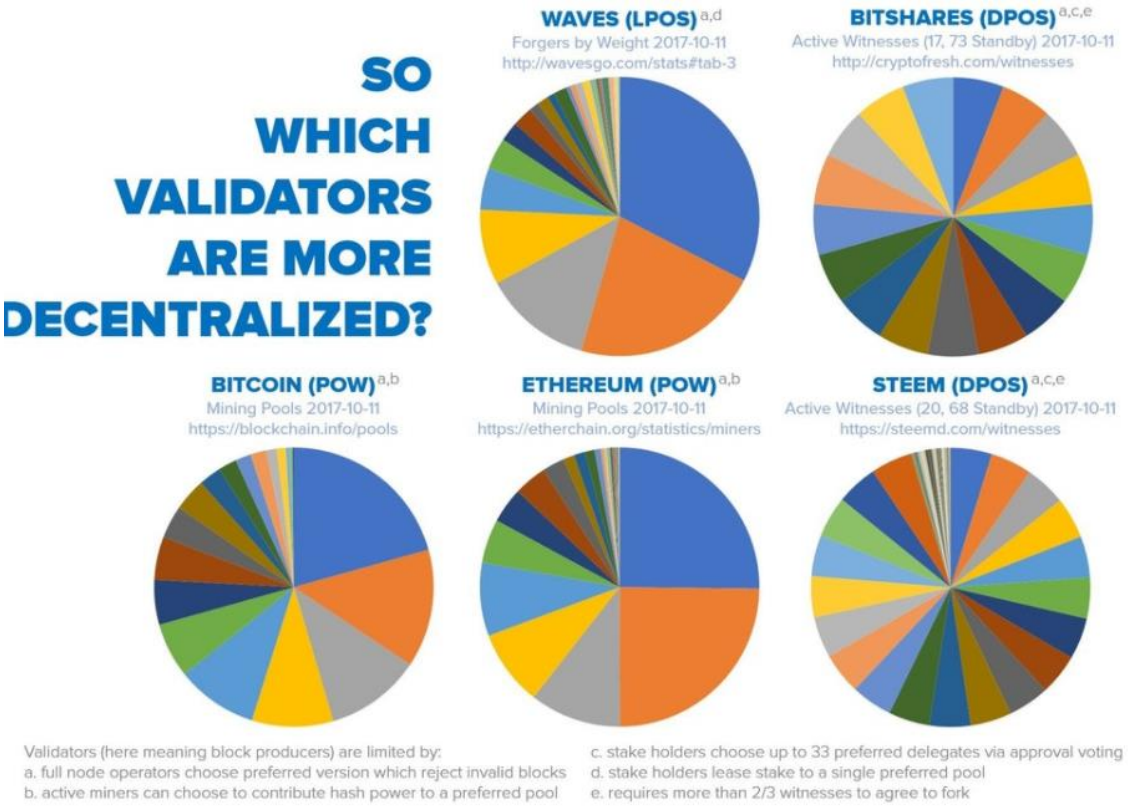
Este voto emitido a determinados validadores de bloques puede ser retirado en cualquier momento, desincentivando por tanto las malas prácticas que puedan tener estos validadores con la red, ya que podemos retirarles nuestro voto en cuestión de segundos. A su vez, estos validadores estarán en constante competencia para convencer a los tenedores de la red de que son la mejor opción.

Por ello, podemos ver a las redes DPOS algo más centralizadas que Bitcoin o Ethereum, a cambio de beneficios como la alta velocidad y la baja latencia, pero manteniendo ciertas medidas de descentralización en su base, con un sistema de

votación y un mínimo número de validadores de bloques que pueden ser expulsados inmediatamente por malas prácticas.

Quizá la pregunta sea cómo podemos medir esa descentralización y si realmente es suficiente, lo cual es la principal razón de crítica hacia sistemas DPOS. Sin embargo, si intentamos medir esta descentralización como un conjunto de variables, es posible que para determinados nichos de mercado DPOS sea el protocolo adecuado. Al fin y al cabo, dependiendo del cometido del protocolo, no podemos tener todo a la vez: resistente al cambio, consenso, participación abierta, inmune frente a ciertos ataques y eliminación de puntos débiles donde se pueda atacar a la red.

Aun así, eventualmente 21 validadores de un sistema DPOS situados en distintas jurisdicciones podrían ofrecer una descentralización bastante alta, incluso tanto como Bitcoin, sobre todo cuando nos encontramos en un punto donde la mayor parte de prueba de trabajo de Bitcoin se lleva a cabo por un grupo muy reducido de “pools” de minería que controlan la mayor parte de la validación de bloques:



Sobre cómo en determinadas circunstancias un sistema DPOS podría ser tan descentralizado o más que un POW como el de Bitcoin, encontramos este interesante post en Steemit: https://steemit.com/eos/@iang/eos-with-dpos-is-immune-to-the-gfw-attack-because-it-is-more-decentralised

Otro de los puntos interesantes del sistema DPOS es que el coste de transacción es cero, es decir, la inflación que genera la moneda es suficiente para incentivar a todos los tenedores y validadores de la misma. Esto hace que los mineros o validadores de bloques en este tipo de sistema no tengan incentivos económicos para generar más bloques o rechazar determinadas transacciones simplemente para poder generar más dinero en concepto de comisión de transacción.

Los bloques en DPOS se producen muy rápido. En STEEM tenemos un nuevo bloque cada 3 segundos, lo cual lo convierte en una de las redes descentralizadas con confirmaciones más rápidas y con coste de transacción cero. EOS, el proyecto basado en DPOS y esperado para mediados de 2018, ha probado en beta hasta 600 transacciones por segundo, aunque se esperan hasta 5.000 transacciones por segundo sin necesidad de estructuras de ejecución en paralelo, donde en un futuro se podrían alcanzar hasta 50.000 transacciones por segundo. Esta última actualización de EOS se resume muy bien en este post: https://steemit.com/eosio/@dan/eos-io-development-update

Estas transacciones gratuitas y eficiencia con baja latencia, rápida confirmación y alta velocidad de la red permiten que de entre las 5 blockchains con mayor actividad (según Blocktivity - https://www.blocktivity.info/) encontremos 3 de ellas que estén basadas en DPOS: STEEM, BitShares y Golos.

#	Name	Activity	Average (7d)	Record	Market Cap	AVI	CUI
1	STEEM	1,677,785 Tx	1,727,008 Tx	2,068,341 Tx	$ 0.519 B	2,240	
2	BTS	866,714 Tx	510,264 Tx	1,472,278 Tx	$ 0.379 B	1,583	
3	ETH	666,094 Tx	677,237 Tx	1,372,918 Tx	$ 59 B	8	
4	BTC	197,762 Tx	188,469 Tx	497,349 Tx	$ 137 B	1.0	
5	GOLOS	100,657 Tx	62,962 Tx	336,089 Tx	$ 0.009 B	7,472	

Donde definen “Activity” como el número de transacciones de la red en las últimas 24 horas. Y lo cierto es que mientras hemos encontrado ciertos colapsos de transacciones en redes como Ethereum o Bitcoin, en redes DPOS como STEEM no han tenido transacciones pendientes y todavía tienen mucho ancho de banda para escalar sin problema.

Resumiendo, en POW los mineros son los que tienen acceso al mejor hardware y la electricidad barata para minar esa criptomoneda, en POS los mineros son los que tienen mayor número de criptomonedas, y en DPOS podemos ver estos mineros como

agentes contratados democráticamente por la mayor parte de la red para realizar el trabajo de validación y generación de bloques.

En los dos primeros casos, si los mineros actúan en su propio beneficio y no en el de toda la red o comunidad, no hay manera de “despedirles”. En cambio, con el algoritmo de DPOS, disponemos de una infraestructura que nos permite expulsar a aquellos validadores que no se estén comportando de forma honesta.

Además de esta gobernanza integrada en el algoritmo, la inflación de la masa monetaria permite que el proyecto tenga siempre fondos para costear su evolución y desarrollo. El gasto energético que se produce con sistemas como POW, en el caso de DPOS se puede utilizar para financiar partes del proyecto que serán votadas por la mayoría, a cambio de renunciar a una descentralización y seguridad del 100%.

Como conclusión, vemos DPOS como una solución práctica al problema de la escalabilidad de blockchains descentralizadas y no permisionadas. Además, ofrece soluciones de gobernanza totalmente integradas en el propio protocolo. En cuanto a la descentralización, creemos que para determinados nichos de mercado esta semi-descentralización de la producción de bloques delegada en n agentes tiene sentido.

Por ello, además de STEEM, EOS es uno de nuestros proyectos favoritos que utilizan DPOS, ya que será una plataforma de contratos inteligentes y aplicaciones descentralizadas, y estamos seguros de que para muchas de esas aplicaciones, DPOS supone una estupenda solución práctica para que puedan escalar.

No esperamos que DPOS sustituya a POW y por tanto a redes como Bitcoin, ya que no se alcanzan los mismos niveles de descentralización y resistencia ante ataques bizantinos, pero a cambio si alcanzamos los niveles de velocidad y eficiencia que necesitan algunas aplicaciones. Por lo que DPOS no solo puede convivir con Bitcoin y con POW, sino que estamos convencidos de que será un mercado que capitalice trillones de dólares en un futuro.

Un saludo,

Román.

Seguimiento de Criptodivisas

- **Bitcoin (BTC)** → Sigue siendo el proyecto más fuerte con más desarrolladores, pero debe superar sus problemas de escalabilidad. Creemos que LN y Segwit tienen potencial para que Bitcoin pueda escalar. Junto con su uso masivo y su función como puerta de entrada desde FIAT, hacen que la sigamos considerando como el protocolo líder. **Criptodivisa con riesgo medio. En un portfolio de criptodivisas, no superamos el 60%**.

- **Ethereum (ETH)** → criptodivisa clave como plataforma base para la generación de contratos inteligentes. **Criptodivisa con riesgo medio. En un portfolio de criptodivisas, no superamos el 40%**.

- **Monero (XMR)** → de todas las alternativas a Bitcoin, este es uno de los protocolos que más nos gustan, ya que ofrece una solución impecable al problema de privacidad en las transacciones. **Criptodivisa con riesgo alto. En un portfolio de criptodivisas, no superamos el 10%**.

- **Dash (DASH)** → otra alternativa a Bitcoin, que ofrece soluciones eficientes en cuanto al problema de confirmaciones instantáneas. **Criptodivisa con riesgo alto. En un portfolio de criptodivisas, no superamos el 10%**.

- **Steem Power (SP)** → sigue siendo nuestra apuesta en el nicho de la generación de contenido descentralizado. **Criptodivisa con riesgo alto. En un portfolio de criptodivisas, no superamos el 10%**.

- **EOS** → plataforma de contratos inteligentes utilizando el algoritmo DPOS (proof of stake). Este algoritmo consigue un buen rendimiento en términos de velocidad y escalabilidad, aunque perdiendo cierta descentralización. **Criptodivisa con riesgo alto. En un portfolio de criptodivisas, no superamos el 10%**.

- **Basic Attention Token (BAT)** → criptodivisa que propone una solución eficiente al mercado de publicidad online. Se puede comprar a través de la casa de cambio Binance, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **Civic (CVC)** → su uso masivo supondría una mejora notable de los procesos de KYC – "Know Your Customer" y todo tipo de mercado relacionado con la identificación de personas. Se puede comprar a través de la casa de cambio

Binance, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **GAS** → alternativa asiática a Ethereum. Cada vez surgen más ICOs sobre NEO y consideramos GAS como la criptodivisa para apostar por esta plataforma en el largo plazo. **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **Zcash (ZEC)** → propone una mejora a Monero con respecto al problema de la privacidad y fungibilidad en criptodivisas como bitcoin. Se puede comprar a través de la casa de cambio Binance, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **Zcoin (XZC)** → propone una mejora a Monero con respecto al problema de la privacidad y fungibilidad en criptodivisas como bitcoin. Se puede comprar a través de la casa de cambio Bittrex, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **0x protocol (ZRX)** → protocolo que propone una solución eficiente para escalar los intercambios descentralizados sobre Ethereum. Se puede comprar a través de la casa de cambio Binance, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

Preguntas y respuestas

Este mes no hay preguntas.

En nuestra sección de Tutoriales encontraréis cuales son las formas más seguras de comprar y almacenar estas criptodivisas. En cuanto al formato de la organización de la página y nuestros informes, si echáis algo en falta en los tutoriales o tenéis cualquier duda o aclaración, no olvidéis por favor en comunicárnoslo en nuestro email: soporte@consultorabitcoin.com

Para nosotros es importante vuestra opinión, para ir adaptando rápidamente la página y así mostraros los contenidos y los manuales que os resulten más útiles. Hemos comenzado un nuevo apartado de **preguntas y respuestas** donde contestar vuestras preguntas de forma centralizada, ya que pueden resultar útiles a otros usuarios. Por favor, al realizar la pregunta decidnos explícitamente si no queréis que publiquemos vuestro nombre.

Gracias,

El equipo de Consultora Bitcoin.
