La verdad es que en tan sólo un mes son tantas las noticias y los eventos que tienen lugar en el ecosistema de las criptodivisas, que parece que han pasado años en el sector.

Antes de entrar en detalle sobre la privacidad, tema en el que hemos querido focalizar el informe de este mes, queremos recalcar la importancia de tener una cartera de criptodivisas concentrada en los proyectos con mayor valor fundamental.

Como sabéis, la idea de esta carta mensual es ofrecer educación sobre los activos digitales que vemos con mayor potencial, para así poder ayudaros a tener carteras que sobrevivan en el largo plazo.

Este ecosistema está en constante cambio, y nos ofrece los activos más volátiles que podamos encontrar ahí fuera. Con ello, aparecen agentes en este mercado que pretenden hacerse ricos con la primera ICO que pasa por delante y en menos de 4 semanas. Como sabéis, no es la idea de este informe, sino más bien todo lo contrario: establecer las pautas para ayudaros a tener posición en criptodivisas sin perder la camisa en el camino.

Los mensajes sensacionalistas son muy fáciles de trasmitir, como el típico titular de un conocido periódico español por el cual muchos hoy conocen el bitcoin: “el joven que invirtió 100 euros en bitcoin y ahora tiene 1 millón”. Conozco a pocas personas que hayan comprado bitcoin por debajo de los 50 dólares, y lo primero que les pregunto no es su rentabilidad, sino como vivieron la caída de bitcoin desde los 1100 dólares hasta los 185 dólares a mediados de 2015. Esa caída de más de 18 meses habría desanimado a cualquiera:

Nos gusta sacar pecho y ser sensacionalistas cuando vemos rendimientos desorbitados, pero desde Consultora Bitcoin creemos que la gestión del riesgo tan importante o más que el mero hecho del rendimiento que consigamos.

Por ello, queremos recalcar nuestro alto porcentaje en cartera de los proyectos más sólidos que encontramos actualmente: Bitcoin y Ethereum. Creemos que es importante tener un alto porcentaje en cartera de ambos. Son muchos los que buscan la piedra filosofal del proyecto que consiga aplastar a Bitcoin y Ethereum, pero no podemos olvidar que eso es muy difícil. En el mundo de la tecnología la capacidad del efecto red es muy potente, por lo que eventualmente se producen monopolios de uno o dos productos para un determinado nicho.

En el mundo del dinero digital esto no será diferente: estamos convencidos que para cada nicho de mercado al final encontraremos tan sólo uno o dos activos digitales a lo sumo que se hagan hueco en esa industria.

Además, es importante tener en cuenta que la principal fuente de revalorización que están teniendo las criptodivisas viene dada por una masiva entrada de capital: euros, dólares, libras… Para esta entrada los mercados más líquidos con respecto a divisas tradicionales los encontramos respecto a Bitcoin y Ethereum, poco más.

Además, el resto de criptodivisas que no son BTC o ETH, normalmente cotizan con respecto a estos últimos, por lo que existe una necesidad de compra de estos activos como “peaje” de acceso a otras criptodivisas menos líquidas. Esto hace que, en eventos de pánico, todo el que quiera deshacerse de estas criptodivisas de menos capitalización obligatoriamente lo tenga que hacer vendiéndolas por ETH o BTC, lo que provoca que BTC y ETH se comporten incluso como activos de “cobertura o refugio” en momentos de pánico de mercado.

Un buen portal donde registrar nuestro “portfolio” y hacer el seguimiento de cómo evolucionan los % de nuestra cartera es https://www.cryptocompare.com/portfolio/

Nos preocupa que el mercado este muy centrado en ese nuevo proyecto que nos va a dar rendimientos estratosféricos y que nos olvidemos de los proyectos más importantes, establecidos, con miles de desarrolladores soportándolos y un ecosistema de empresas y servicios por detrás que empieza a contabilizarse en billones (americanos) de dólares.

Esto no quiere decir que desde Consultora Bitcoin no estemos constantemente examinando posibles competidores y tecnologías nuevas que tengan probabilidades de desbancar a estos proyectos, pero siempre apostando en concordancia.

Esto es, si por ejemplo tenemos una cartera de criptodivisas con un 30% en ETH, creemos que no debemos dedicar más de un 5% de la cartera a ideas que se

presentan como competidores en el sector de los contratos inteligentes: EOS, NEO, BOSCoin, etc.

En definitiva, ya son más de 1100 activos digitales los que podemos encontrar ahí fuera, y estamos convencidos de que el ratio de supervivencia de estos proyectos será muy bajo. En el largo plazo esperamos que tan sólo un 20% de todos los activos digitarles sobrevivan, de los cuales unos pocos se harán con el monopolio para determinados nichos.

Por ello, ahora más que nunca, tenemos que ser muy selectivos. Nosotros cada vez que analizamos un nuevo proyecto o ICO lo primero que pensamos es lo siguiente: "veamos cómo me venden la moto para robarme mis preciados ETH o BTC".

No dejéis de visitar el apartado de preguntas frecuentes, y por favor realizad las vuestras en nuestro buzón: soporte@consultorabitcoin.com También podéis solicitar la inclusión de cualquier tutorial que echéis en falta.

Monero – La privacidad importa

Una de las propiedades de blockchain que conseguirán cambiar el mundo en el que vivimos es la transparencia. La mayor parte de los protocolos sobre blockchain, entre ellos bitcoin, son totalmente transparentes. Una vez que conozco cuál es tu clave pública, automáticamente podemos sacar todas las transacciones enviadas y recibidas desde esa clave pública.

El explorador de claves más utilizado para la red de Bitcoin es https://blockchain.info/ y el más utilizado en la red de Ethereum es https://etherscan.io/ . En ambos buscadores podéis introducir cualquier clave pública de la red o código de transacción y obtendréis toda la información de ese monedero en segundos.

Por ello, podemos decir que Bitcoin es pseudónimo, no anónimo, y con ello se pierde una de las propiedades más importantes del dinero en efectivo: la privacidad. Desde Consultora Bitcoin pensamos que el nicho de mercado de la privacidad es muy importante dentro y fuera de la industria blockchain. El efectivo es el método de pago privado entre personas que ha existido siempre, y estamos seguros de que eso no va a cambiar.

La primera solución real a la privacidad de un protocolo blockchain la encontramos con Monero. Monero es un protocolo que permite el envío de criptodivisas con un algoritmo

que mantiene el anonimato del emisor de la transacción, ya que todas las transacciones efectuadas en el mismo bloque serán mezcladas varias veces, y así la emisión y recepción del dinero digital será totalmente caótica, y por tanto privada.

Con un ejemplo práctico, imaginemos que hago una transacción de 1 monero a Pepe. Al final de ese bloque Pepe tendrá su monero, pero no parecerá que se lo he enviado yo, ya que recibirá numerosas transacciones de particiones aleatorias de moneros que se han estado enviando al mismo tiempo que yo enviaba ese monero a Pepe.

Esto hace que, a diferencia de bitcoin, monero sea una moneda 100% fungible. La fungibilidad no es tan sólo el hecho de que una divisa se pueda particionar, sino que cada una de las particiones tenga exactamente el mismo valor independientemente del camino que haya recorrido.

En el caso de los euros, seguro que más de uno ha puesto mala cara cuando le devolvían como cambio en la gasolinera ese billete de 5 euros asqueroso y roto por todas partes. Imaginemos un supuesto caso donde al margen de la apariencia física del billete, con tan solo meter el código del billete en una página web, supiéramos por cuántas manos de delincuentes y drogadictos hubiera pasado.

Esto en el mundo de los billetes de 5 euros es una tarea ardua e impracticable. Sin embargo, en el mundo bitcoin, gracias a su transparencia, ya hay empresas que se empiezan a dedicar exclusivamente a investigar toda la traza que deja un bitcoin, con todo lo que ello conlleva. Cuanto más precisas y rápidas sean estas herramientas que siguen la traza de un bitcoin, menos fungible será la criptodivisa, ya que distintas trazas pueden dar lugar a distintos valores de particiones: es posible que un bitcoin que haya pasado por determinadas “manos” no sea aceptado por determinado tipo de empresas, sujetas a una regulación.

Monero, además, mejora en términos de escalabilidad, ya que sus bloques no están limitados a 1Mb, adaptándose a las necesidades de su blockchain. Otra de sus ventajas es la dificultad de minado de la moneda utilizando hardware específico. Es decir, hoy en día minar bitcoin es un proceso complejo donde tan sólo unas pocas asociaciones o “pools” de minería con hardware muy específico y caro están llevando a cabo.

La idea original de Satoshi estaba enfocada a 1PC = 1nodo, ya que su escrito original proponía que todos los dispositivos que usaran la red también la minarían para mantenerla segura y estable. Hoy en día sabemos que no es así, la minería de bitcoin está centralizada en unos pocos, en comparación con los millones de usuarios de Bitcoin que se reparten por todo el mundo.

Con divisas como Monero, el minado con un PC normalito todavía tiene sentido, lo cual hace que sea una divisa más descentralizada y por tanto muchísimo más difícil de

corromper (de ahí las noticias sobre hackers usando ordenadores de empresas para minar monero; así que cuidado con tu ordenador, es posible que haya algún hacker minando monero con él). Sin embargo, hay que decir que actualmente 3 pools de minería controlan más del 40% de la potencia de cómputo de la red de Monero.

Las transacciones en Monero son privadas gracias a este barajeo de cartas utilizando el llamado anillo de firmas o "ring signature". El número de monederos involucrados en este barajeo también dependerá de la comisión que se pague por la transacción: cuanto más alta sea más direcciones estarán involucradas en este barajeo o mezcla de transacciones entre todas ellas.

En definitiva, Monero es un proyecto que seguimos monitorizando y nos gusta desde hace tiempo. Está en nuestra lista de seguimiento de criptodivisas desde el comienzo de esta publicación, cuando monero cotizaba algo por encima de los 40 dólares. Como sabéis, Monero se puede comprar a través de Kraken y su símbolo es XMR.

Zcoin – ¿Es Monero 100% privado?

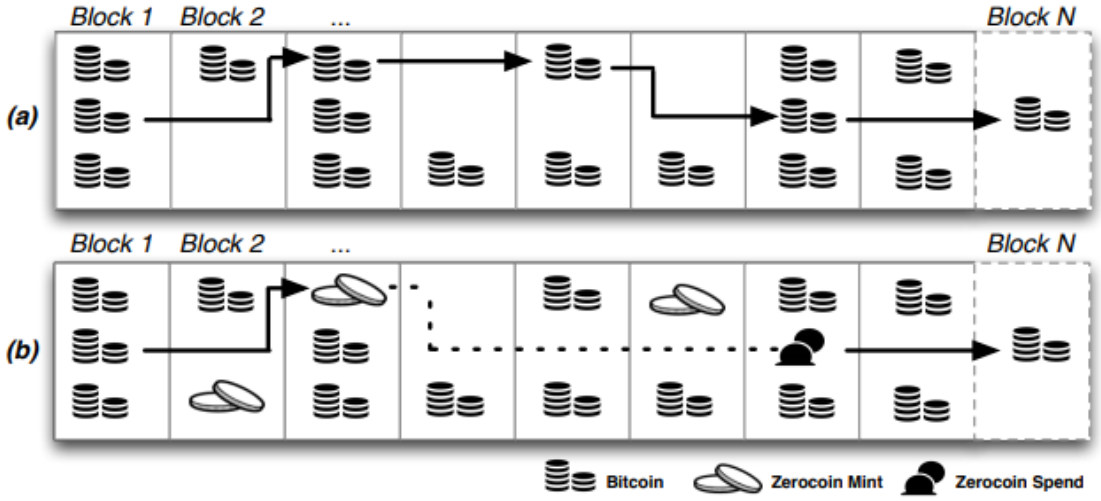
Zcoin es un proyecto muy joven. Comparado con Monero, tiene muchos menos desarrolladores y capital que lo avale, por lo que es un proyecto mucho más arriesgado.

Sin embargo, nos ha convencido la calidad de su equipo, centrado en la matemática que hay detrás de su algoritmo, proponiendo una mejora a Monero en términos de privacidad.

¿Cuál es el problema que ven detrás de Monero? Creen que para determinadas transacciones podría haber complejos algoritmos que rastreen todo ese barajeo de cartas, descubriendo patrones de gasto y por tanto desvelando ciertas transacciones, tanto usuarios como cantidades.

Su propuesta es compleja: en lugar de barajar todas las transacciones durante un bloque, ¿qué tal si directamente generamos las monedas a gastar por Pepe en un nuevo bloque y efectuamos el envío?

Esta propuesta tiene su base en el "paper" de Zerocoin. Para los amantes de la criptografía y las mates, podéis seguir el razonamiento en el siguiente link: http://zerocoin.org/media/pdf/ZerocoinOakland.pdf



Por tanto, la tecnología de Zcoin permite no sólo enviar de forma privada, sino evitar cualquier tipo de búsqueda de patrones en ese barajeo aleatorio que realiza Monero.

No queremos confundiros: desde Consultora Bitcoin consideramos que el algoritmo de Monero soluciona perfectamente el problema de privacidad de Bitcoin. Sin embargo, estamos atentos a posibles mejoras que puedan ofrecer otros protocolos, en este caso Zcoin, el cual consideramos interesante y con gran atractivo a estos niveles de capitalización.

Podéis encontrar Zcoin (XZC) en Bittrex. Para comprar, por favor seguid los tutoriales de Bittrex paso a paso.

https://coinmarketcap.com/currencies/zcoin/#charts

Seguimiento de Criptodivisas

- **Bitcoin (BTC)** → tenemos el posible hardfork de Bitcoin Gold para el 25 de Octubre y el hard fork de Segwit2X para Noviembre (ya planeado desde el famoso NYA – "New York Agreement"). Que no cunda el pánico. Importante mantener los bitcoin en wallets donde seamos dueños de la clave privada o en exchanges que soporten los forks. Os mantendremos informados las próximas semanas. **Criptodivisa con riesgo medio. En un portfolio de criptodivisas, no superamos el 60%**.

- **Ethereum (ETH)** → ya se está probando en la testnet de Ethereum la nueva versión Metropolis. Esta conseguirá mejorar la escalabilidad de la red de Ethereum, simplificar la programación en Solidity e incrementar la dificultad de minado, lo cual hará que la inflación de la criptodivisa (ya de por sí baja) disminuya considerablemente. **Criptodivisa con riesgo alto. 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%**.

- **Steem Power (SP)** → STEEM nos sorprende una vez más lanzando los Smart Media Tokens, nuevo activo digital vinculado a STEEM que permitirá monetizar comentarios por parte de otros gestores de contenido. Podéis ver el "paper" con toda la información en el siguiente link: https://smt.steem.io/ . **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 Bittrex, 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 Bittrex, utilizando bitcoin (BTC). **Criptodivisa con riesgo MUY alto. En un portfolio de criptodivisas, no superamos el 5%**.

- **EOS** → la consideramos interesante para cubrir parte de nuestra posición en Ethereum mientras ésta soluciona sus problemas de escalabilidad.

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 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%**.

Preguntas y respuestas

Pedro (Madrid) → *Si queremos comprar bitcoin, ¿es mejor hacerlo ya o esperar al 25 de Octubre tras el nuevo hard fork?*

Mi respuesta quizá te parezca demasiado simple: siempre es un buen momento para comprar bitcoin. A partir de ahí, es cierto que determinados indicadores pueden ayudarte a comprar en un mejor momento o más barato.

La última vez que tuvimos un hard fork en bitcoin el precio estuvo estable y comenzó a subir fuertemente durante las siguientes semanas. ¿Volverá a pasar lo mismo? No lo sabemos; y la muestra es insuficiente (solo 1 muestra). Por ello, considero más interesante la compra sistemática (x cantidad fija al mes sin importarme el precio) o acumular cuando tengamos correcciones o situaciones de extremo pesimismo: China prohíbe bitcoin, JP Morgan dice que bitcoin es un fraude, atacan a un exchange, etc…

Jorge (Madrid) → *Charlando con un amigo, me insiste que Bitcoin es un invento que no está respaldado por ningún Estado o bien físico, y por tanto su valor es mera especulación, ¿qué le puedo decir?*

En cuanto a que bitcoin es un invento, tu amigo tiene razón. Es un algoritmo de software totalmente libre que puedes instalar en tu casa: instalas un nodo en el baño, otro en la cocina, lo llamas BitcoinJorge y empiezas a enviarte BitcoinJorge del baño a la cocina hasta que te canses. Luego sí, es un invento.

También es cierto que no está respaldado por ningún Estado o bien físico, pero esto lo considero una ventaja de bitcoin: está totalmente descentralizado, y por tanto no hay entidad pública o privada que pueda comprarlo o corromperlo.

Es la última parte de la afirmación de tu amigo la que es algo incorrecta: "su valor se basa en mera especulación". Con respecto a esto hay una frase en política que me encanta: "*puedes engañar a todo el pueblo por un tiempo; también puedes engañar a parte del pueblo todo el tiempo; sin embargo,* ***no puedes engañar a TODO el pueblo TODO el tiempo***". Si Bitcoin no tuviera valor, con tantas idas y venidas desde 2009, estaríamos entrando en esta última parte en la que nos estarían engañando a TODOS durante TODO el tiempo.

Pero quiero contestar más directamente a tu pregunta: ¿cuál es el valor de Bitcoin? ¿Por qué el blockchain de Bitcoin tiene más valor que el BitcoinJorge que me he instalado en casa?

Su valor es el efecto red: son millones de usuarios los que están utilizando actualmente este protocolo para enviar y recibir transacciones a través de la red. Me gusta pensar en Bitcoin como si fuera una increíble autopista con 3 carriles de ida y de vuelta. bitcoin sería el peaje que tenemos que pagar por utilizar tal autopista. Y, ¿por qué iba a utilizar esa autopista? Quizá porque todas las alternativas son carreteras comarcales de montaña y vayas a duplicar tu tiempo en carretera, y por tanto te compensa el pago del peaje.

Por lo tanto, el valor de Bitcoin se basa en la calidad de su autopista, su protocolo, y su red de uso, que actualmente es la ganadora de entre todas las blockchains, con cientos de miles de comerciantes y transacciones diarias en todo el mundo.

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 vuestro feedback 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.

Hasta el próximo mes.

Un saludo,

Román.