ANEXOS

"Las criptomonedas, el blockchain y su comparativa con las divisas"

"Cryptocurrencies, the blockchain and its comparison with currencies"

Autor/es

Sergio Giménez Gil

Director/es

Aurora Sevillano Rubio

Facultad de Economía y Empresa de la Universidad de Zaragoza
2021

ÍNDICE DE ANEXO

ANEXO 1. Principales modalidades de Blockchain

Las redes de blockchain se pueden clasificar como redes públicas o privadas. Las redes públicas se caracterizan por la ausencia de restricciones por parte de los usuarios para acceder a los datos de la red, mientras que las redes privadas tienen la condición de tener un acceso a la lectura de los datos de la red a participantes determinados (Parrondo, 2008)[1].

La primeras blockchains fueron diseñadas con el objeto de que tuvieran cuatro atributos esenciales, públicas, abiertas, descentralizadas y pseudoanónimas. Las blockchain públicas son por definición "una red descentralizada de ordenadores que utilizan un protocolo común asumido por todos los usuarios y que permite a éstos registrar transacciones en el libro mayor de la base de datos". Por su parte, las blockchain privadas surgen como consecuencia de la posibilidad que ofrece la propia tecnología blockchain de establecer características distintas estando justificado en el hecho de que no se puede compartir, por razones regulatorias o de confidencialidad, sus bases de datos de forma abierta (Preukschat, 2017)[2]. Así, podemos clasificar la tecnología blockchain en tres tipos atendiendo a las decisiones que se haya producido sobre la transparencia, la irrevocabilidad y la inmutabilidad.

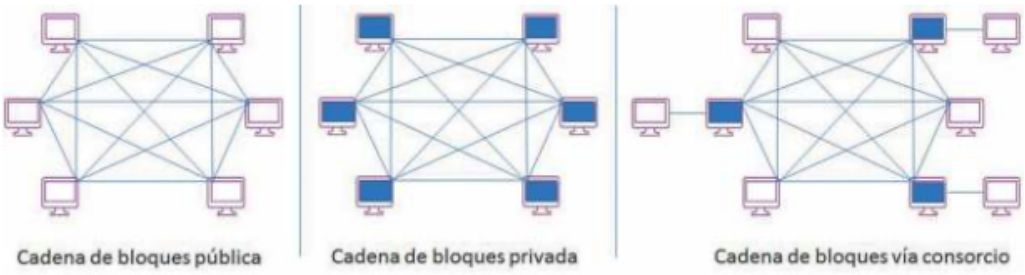
- ***Blockchain públicas:*** se caracterizan por la ausencia del cumplimiento de requisitos por parte de los usuarios para poder unirse a la red y la no existencia de ningún tipo de jerarquía entre los nodos o participantes, de forma que cualquiera de los nodos que participen en la red puede convertirse en validador si quiere. Otro aspecto esencial sería la transparencia y la visibilidad del contenido de la cadena de bloques, incluso por usuarios que no forman parte de la red. Debido a la ausencia de permiso o invitación para poder participar en la red este tipo de redes reciben el nombre de *"permisionless"* (Menéndez, 2018)[3].

[1] LUZ PARRONDO, "Tecnlogía blockchain, una nueva era para la empresa". Revista de Contabilidad y Dirección. Vol. 27, año 2008, pp 12- 16
[2] PREUKSCHAT, A. "Blockchain: La revolución industrial de internet". Barcelona, 2017.
[3] URÍA MENÉNDEZ, "Tecnología Blockchain: Funcionamiento, Aplicaciones y Retos Jurídicos Relacionados". Actualidad Jurídica Uría Menéndez. 2018.

- ***Blockchain privadas:*** en este tipo de redes, sólo un grupo limitado de actores conserva el poder de acceder, comprobar y añadir transacciones al libro de registro (Boucher, 2017)[4]. En estas redes el control lo tiene una entidad la cual tiene como labores esenciales el mantenimiento de la cadena, otorgar los permisos necesarios para que los participantes entren en la red, proponer transacciones y aceptar los bloques. Vemos que tienen una característica diferencial con respecto a las públicas, pierden la descentralización.

- ***Blockchain híbridas:*** en este caso se tratan de redes que ostentas características tanto de las redes privadas como de las públicas. Se caracterizan por el hecho de que un número determinado de entidades son las encargadas de administrar la red, de forma que la entrada en esta red por parte de los potenciales participantes debe ser aceptada por la totalidad de entidades que administran la red.

Imagen 1. Tipos de cadenas de bloques[5]



Fuente: Lin y Lao. 2017

[4] BOUCHER, P: «How blockchain technology could change our lives», In-depth Analysis, European Parliamentary Research Service, Febrero 2017, pág. 5

[5] JEIMI.J. "Blockchain: Cadena de bloques. Reflexiones sobre seguridad y control".Revista SISTEMAS. 2017. Pg 48.

ANEXO 2. Tipos de Carteras o Wallets

- ***Carteras frías (Hardware):*** Se tratan de dispositivos que almacenan la cartera de un usuario a través de un hardware fuera de línea (por ejemplo, un dispositivo USB), lo que otorga gran seguridad. En este tipo de carteras, la clave privada se encuentra en el interior de un microcontrolador y no puede ser transferida. Este tipo de carteras son las únicas que suponen un coste directo para el tenedor, ahora bien, el nivel de seguridad que otorgan es mayúsculo. Las más reconocidas a nivel mundial son Keep Key, Trezor, Case y Ledger Wallet.

- ***Aplicaciones de carteras (Software):*** Se tratan de softwares que se encuentran instalados en un ordenador o en un móvil teniendo la función de servir de interfaz que permita al usuario ver los saldos en las direcciones que posee y mover el dinero en ellas. Pueden insertarse códigos extra para la movilización del dinero. Este tipo de cartera permite la totalidad disponibilidad del dinero por parte del usuario, pero también es el usuario el que tiene la responsabilidad de guardar la seguridad del dispositivo. Algunas de ellas son Exodus, Electrum o Bitpay.

- ***Carteras en línea:*** Se trata de sitios web que habilita a los usuarios a mover su dinero de forma independiente sin necesidad de instalar ningún software. Estas carteras se caracterizan porque son los usuarios quienes tienen el control exclusivo de sus claves privadas, generándose una abstracción de la misma que recibe el nombre de semilla. Esta semilla consiste en 12 o más palabras que el usuario debe anotar en un papel y asegurarse de no extraviarlo, pues en caso contrario perdería su dinero. Las más utilizadas en este caso son Blockchain.info y MyEtherWallet.

- ***Casas de cambio (Bancos):*** En este tipo de cartera, los usuarios depositan sus criptomonedas en una dirección y es el "banco" el que se encarga de realizar todas las operaciones (instrucciones de pago, compra o venta) que son ordenadas por los usuarios. Es decir, es el "banco" el que gestiona las criptomonedas de los usuarios. Son adecuados para el intercambio entre criptomonedas y monedas fiduciarias, pero el riesgo de hackeo o estafa es elevado. Algunas de las casas de cambio más utilizadas son Coinbase, Poloniex o Bittrex, entre otros.

ANEXO 3. Principales Altcoins

- **Ethereum:** Ethereum no es en sí una moneda, sino que es una red distribuida descrita por primera vez en 2013 por Vitalik Buterin[6]. El Ether, la moneda que alimenta esta red se utiliza para almacenar valor, que puede estar vinculado a los llamados contratos inteligentes. Estos contratos son acuerdos digitales, almacenados en la cadena de bloques, que permiten intercambiar una variedad de servicios por Ether. Entre los servicios que se pueden intercambiar encontramos recursos computacionales, almacenamiento, mercados de predicción y otros servicios digitales. Actualmente, Ethereum es el segundo valor después del Bitcoin, la cual utiliza al igual que Bitcoin una cadena de bloques (Blockchain) accesible al público, que permite que los valores de las carteras, las transacciones y los contratos se observen libremente.

- **Ripple:** Es una empresa privada que desarrolla softwares para bancos, ostentando su propia criptomoneda XRP. El objetivo de esta plataforma es facultar para realizar transacciones rápidas y baratas a través de un protocolo de código abierto. Empresas como el Banco Santander están utilizando esta plataforma como tecnología de infraestructura de liquidación ya que ofrece una velocidad de pago excelente dentro de la red, además de otorgar estabilidad a la tecnología y la posibilidad de utilizar su moneda como moneda puente.[7]

- **LiteCoin:** Litecoin es considerada como la plata de las criptomonedas, donde Bitcoin es el oro. Consiste en una criptomoneda que permite la realización de pagos instantáneos y coste prácticamente nulo a cualquier lugar del mundo. Tiene una gran importancia en términos de número de transacciones por segundo ya que, mientras Bitcoin únicamente puede realizar 7 transacciones por segundo y Ethereum 15 transacciones por segundo, LiteCoin es capaz de soportar un máximo de 56 transacciones por segundo. El objetivo primordial de esta moneda es servir de sustituto a los pagos con VISA, aunque todavía se encuentra lejos de

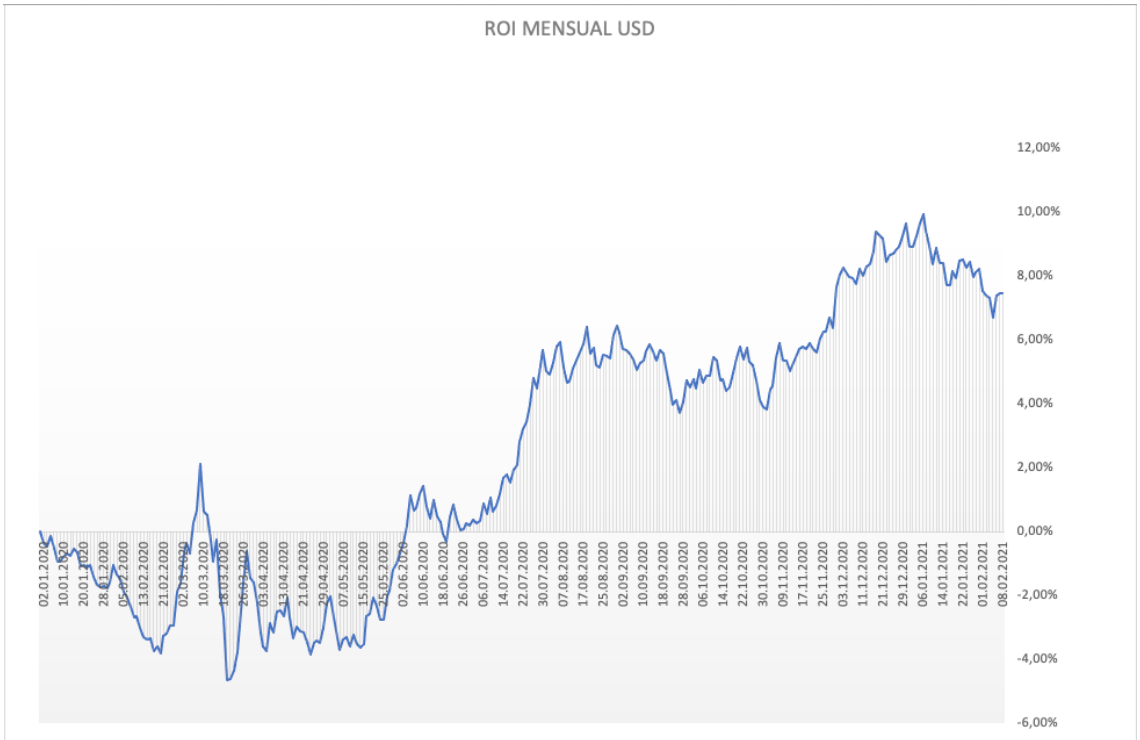
[6] Hernandez- Castro, J. Darren Hurley-Smith. (2017) ALTCOINS: ALTERNATIVE TO BITCOIN AND THEIR INCREASING PRESENCE IN MALWARE-RELATED CYBERCRIME.
[7] https://es.cointelegraph.com/ripple-101/what-is-ripple

hacerlo pues está en una fase muy temprana de desarrollo y los consumidores no tienen confianza en este medio de pago.

ANEXO 4. Evolución ROI mensual en la inversión en Bitcoin y en FOREX (USD)

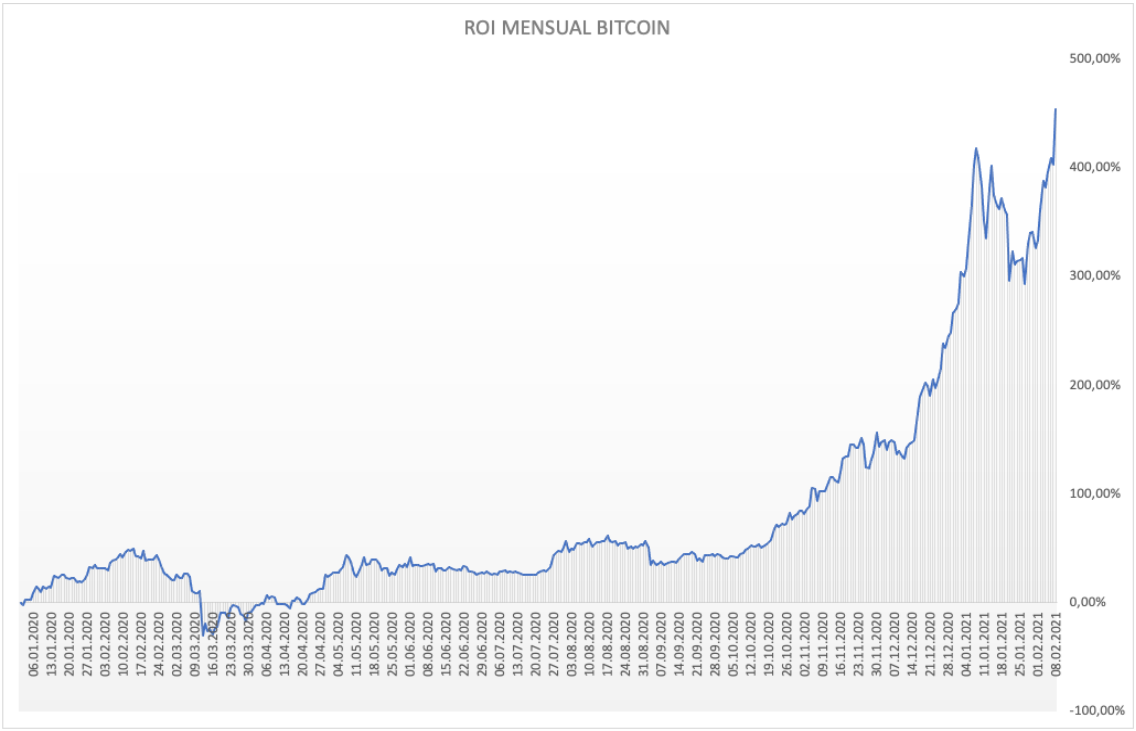
Veamos qué ocurre si invertimos en FOREX y en Bitcoin hace un año, es decir, el 1 de enero de 2020. Una fecha más cercana a la actualidad nos permite vislumbrar mejor las tendencias de ambos mercados.

Imagen 2. ROI mensual inversión en USD



Fuente: Elaboración Propia a partir de datos de Investing.com

Imagen 3. ROI mensual inversión en Bitcoin



Fuente: Elaboración Propia a partir de datos de Investing.com

A la luz de los gráficos vemos que la rentabilidad obtenida con el Bitcoin es inmensamente mayor que en FOREX, alcanzando valores cercanos al 500% en 1 año, mientras que en con la adquisición de USD apenas obtendríamos un valor del 8% de rentabilidad.

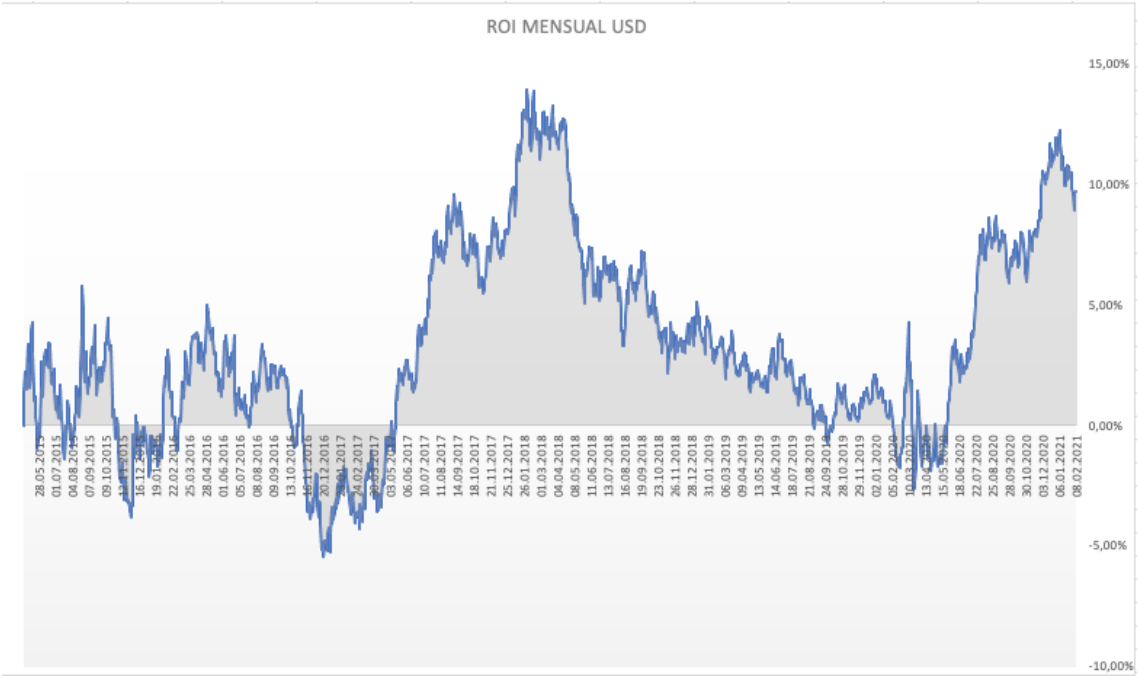
Para una mayor profundidad en el análisis he procedido al cálculo de la rentabilidad mensual en el periodo enmarcado entre el 28 de abril de 2015 y el 8 de febrero de 2021 de ambos activos (Este intervalo de tiempo es adecuado pues es lo suficientemente amplio para comparar ambas inversiones y, además, no se tienen datos anteriores de la cotización del Bitcoin). Los datos para el cálculo de esta rentabilidad los he obtenido de Investing.com. Para el cálculo de esta rentabilidad mensual he utilizado la fórmula del ROI:

ROI = (Valor Final de la Inversión – Valor Inicial de la Inversión) /Valor Inicial de la Inversión

Una debilidad del ROI es que no se tienen en cuenta el plazo del tiempo en el que se tiene la inversión, siendo el tiempo uno de los factores clave para decidir entre una inversión u otra. Para amedrentar este hecho he calculado el ROI anualizado con la siguiente fórmula, teniendo en cuenta que el plazo de tiempo que mantenemos la inversión es de 4,14 años aproximadamente (1511 días):

$$\text{ROI anualizado} = (1+\text{ROI})^{1/n} * 100$$

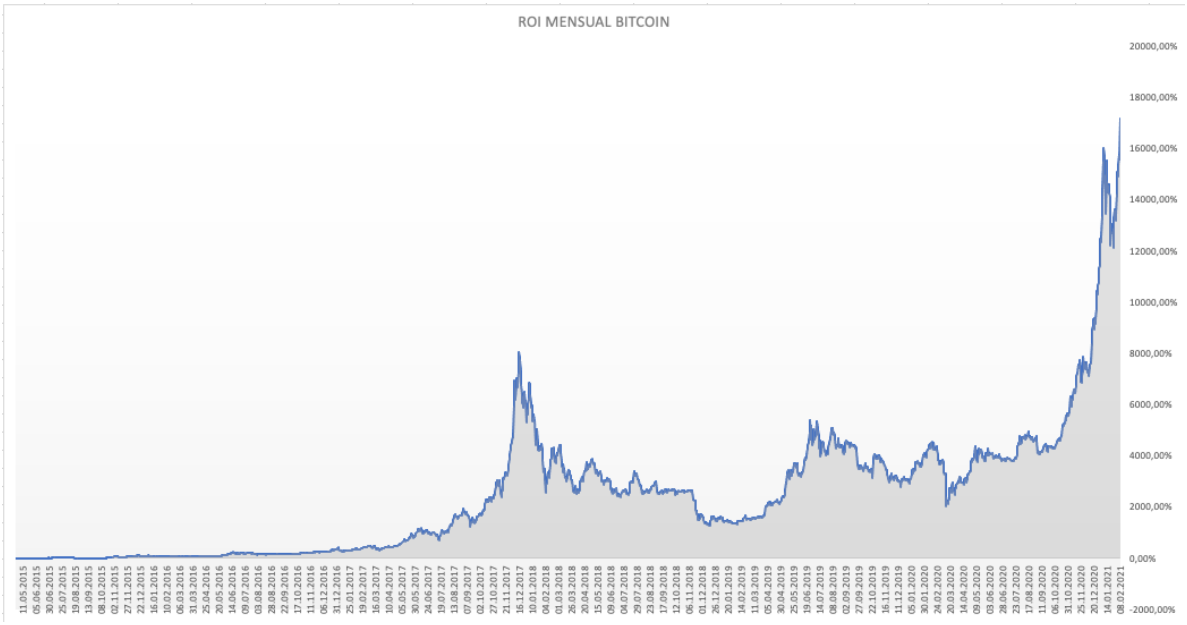
Imagen 4. Evolución rentabilidad mensual invertir en FOREX (USD)



Fuente: Elaboración propia a partir de datos de Investing.com.

Con respecto a la inversión en el mercado FOREX, vemos que la tendencia de la rentabilidad no es uniforme, produciéndose grandes incrementos y decrementos a lo largo del tiempo. Pero el hecho más importante, y que sin duda nos permite llegar a una conclusión es su tasa de rentabilidad. El máximo que se obtendría sería en 2018 con un valor cercano al 15%. Habría sido un momento muy bueno para vender los dólares. Suponiendo que mantenemos la inversión hasta el 8 de febrero de 2021, la ROI sería de un 9,7%. Teniendo en cuenta el plazo de tiempo de la inversión, la ROI anualizada alcanzaría el valor de 26,50%. Estos valores, aunque son positivos para nuestros intereses, distan mucho de la rentabilidad que es capaz de ofrecer bitcoin como veremos a continuación.

Imagen 5. Evolución rentabilidad mensual invertir en Bitcoin



Fuente: Elaboración Propia a partir de datos de Investing.com

Como vemos en los datos de la gráfica, la inversión en bitcoin tiene una tendencia claramente alcista a lo largo del tiempo. El ROI de la inversión alcanza el espléndido valor de 17161% de la inversión inicial, mientras que el ROI anualizado es de 347,05%. Resultados esperados debido a la conocida rentabilidad del Bitcoin. Ahora bien, como en todas las inversiones, una mayor rentabilidad entraña mayor riesgo. La volatilidad del Bitcoin hace que la inversión no presente unos niveles de seguridad aceptables. Hecho que, como hemos colegido no ocurre en el caso de la inversión en el mercado FOREX.