Mercados de criptomonedas y contratos inteligentes

Gustavo Arellano

abril de 2022

Twitter: @arellano_gus

Introducción

- En la antigüedad, el intercambio de objetos o servicios por otros objetos o servicios “equivalentes” establecía un modelo económico de comercio que presentaba dificultades para la realización de transacciones justas y uniformes entre las partes que no siempre estaban de acuerdo con la equivalencia de los productos o servicios a intercambiar.
- De lo anterior, surge la necesidad de la creación de un sistema de intercambio “relativo o indirecto”, que proporcione un instrumento a través del cual el valor de cada producto o servicio pueda ser equiparado con fragmentos de otro producto o servicio.
- Las primeras monedas acuñadas con carácter oficial fueron hechas en Lidia, (hoy una región de Turquía), aproximadamente entre los años 680 y 560 a. C.
- Desde entonces, el “dinero” es tan codiciado, aunque no es posible “comerlo” o “vestirse con billetes”. La producción de un billete de 200 cuesta lo mismo que la de un billete de 100 pero el primero vale el doble… ¿porqué?

Moneda del siglo VI a. C. 1/3 de Estátera: anverso y reverso.

Tetradracma de Atenas, siglo V a. C. En el anverso, efigie de Atenea, diosa epónima de la ciudad. En el reverso, la lechuza de Atenas.

Sistema bancario antiguo

- Aunque el concepto de “préstamo” y “rendimiento del préstamo” es anterior a la creación de las monedas, con el advenimiento de éstas últimas, la figura de “Banco” comienza a tomar fuerza y se consolida en Italia, durante la Edad Media.
- El mundo antiguo se percata de que la acumulación de activos (monedas) es muy conveniente y mucho mas práctico que la acumulación de animales o comida con la sola desventaja de que las monedas por si mismas no son comestibles y su valor reside (**única y exclusivamente**) en lo que potencialemnte puede ser intercambiado por ellas.
- Adicionalmente, una moneda tiene que ser muy dificil de falsificar y muy dificil de ser legítimamente generada. Por eso, eran generalmente acuñadas en oro.

Modelo comercial reciente

- Aunque por siglos las monedas fueron el instrumento preferente para la realización de transacciones comerciales, en tiempos relativamente recientes nuevos instrumentos aparecieron. Entre ellos están, por ejemplo, los Cheques, las Tarjetas plásticas, Las transacciones totalmente electrónicas, etc.
- A diferencia del instrumento “moneda”, los nuevos instrumentos requieren de un operador que sirve de intermediario para asegurar la integridad de la transacción. Tal operador ha sido desde un empleado que supervisa la validez de un cheque, hasta un sistema automático que garantiza la suficiencia de fondos del emisor y que garantiza la entrega de recursos al destinatario, a cambio de una comisión como compenzación a su intermediación financiera.

Problemáticas que emanan de una gestión central

- Cuando un banco es el único actor que tiene la capacidad de mover recursos entre sus clientes, también tiene la capacidad para auditar cada transacción y de retener los fondos de alguno de sus clientes incluso aun si el cliente no está de acuerdo con tal retención.
- Bajo ciertas circunstancias, un Banco puede establecer comisiones arbitrarias o exageradas para cada uno de sus servicios. Y puede limitar las cantidades de dinero que un cliente puede retirar en un cierto momento.
- En casos extremos, un banco puede ir a la bancarrota con pérdidas y cosecuencias negativas para sus clientes.

Satoshi Nakamoto & Bitcoin Network

- El 31 de Octubre de 2009 un artículo (de sólo 9 páginas) llamado: “Bitcoin: A peer-to-peer Electronic Cash System” (https://bitcoin.org/bitcoin.pdf) abre la posibilidad de eliminar intermediarios financieros abusivos centralizados (Bancos) y propone un mecanismo “abierto” que transparenta y garantiza la totalidad de transacciones entre pares en la red Bitcoin sin la posibilidad de fraude, doble gasto (double spending) o pérdida para alguna de las partes.
- En la red Bitcoin, cada participante posee un tipo de llave pública y una llave privada.
- También existe una emisión inicial de 21 millones de Bitcoins que no cambiará jamás.
- Adicionalmente, existe un conjunto de “nodos” que validan una transacción cuando un participante emplea su llave privada para enviar un monto de Bitcoins a otro actor. Los nodos reciben una recompensa (proveniente de la emisión original de 21 millones) por validar la transacción.

Valor del Bitcoin (sólo usaré 2 láminas para esto)

- Inicialmente (2009) cada Bitcoin tendrá un valor (en dólares americanos) cercano a cero.
- En **marzo** de 2010 el usuario “SmokeTooMuch” subastó en eBay la catidad de 10,000 bitcoins por un precio inicial de 50 dólares americanos. Lamentablemente nadie se interesó por la puja mínima.
- El 25 de **abril** de 2010 la casa de intercambio “BitcoinMarket” estableció el precio de venta en 0.003 centavos de dólar por Bitcoin. (63,000 dólares hubiera costado comprar la beta completa de 21 millones de bitcoins)
- El 22 de **mayo** de 2010 Laszlo Hanyecz pagó 10,000 Bitcoins a una persona que le envió 2 Pizzas “Grandes” a su casa.
- En ese entonces 10,000 Bitcoins estaban valorados en 40 dólares, pero el comprador aprovechó una oferta de Papa John’s y ambas pizzas le costaron 25 dolares. En esa fecha cada dólar costaba 12.31 MXN, por lo que su inversión total fue de 307.65 MXN

laszlo
Full Member

Activity: 199

Re: Pizza for bitcoins?
May 21, 2010, 09:33:45 PM

I just think it would be interesting if I could say that I paid for a pizza in bitcoins

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

laszlo
Full Member

Activity: 199

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

El 26 de Diciembre de 2017, sólo 7 años después, el valor 1 Bitcoin era de 19,872.92 USD
O sea que el valor de 10,000 bitcoins ese día era de 198,729,271 dólares.
Es decir, un poco más que 4,000 millones de pesos Mexicanos.

Cómo funciona el Bitcoin y qué es el Blockchain???

- Cuando un interesado decide comprar Bitcoins, el efectivo en la moneda origen (dólares, por ejemplo) es depositado a una cuenta bancaria regular (Bancomer, por ejemplo) y el poseedor de Bitcoins transfiere de su cartera de bitcoins (usando su llave privada) el monto acordado de la cryptomoneda a la cartera del comprador que previamente le compartió su llave pública (también conocida como cuenta de depósito).
- La transferencia no se hace efectiva hasta que el 50% +1 de los nodos validadores confirman la transacción realizando los siguientes pasos cada uno de ellos:
  - Validar que la cuenta destino existe
  - Validar que la cuenta de Bitcoins origen tiene fondos
  - Realizar una PoW (Proof Of Work) que demuestra que el nodo tuvo que realizar “mucho trabajo” al resolver un problema que requiere gran cantidad de cálculos para ser resuelto.

Blockchain

- Cuando la transacción ha sido validada por el número de nodos requerido, el ID (current_id) de la transacción recién validada se transforma en: `current_id = hash256(current_id + prev_id)`
- Donde `prev_id` es el ID de la transacción anterior.
- Esto provoca un “encadenamiento” de bloques (o más bien de los ID’s de los bloques) desde el bloque inicial hasta el último bloque.
- Es importante hacer notar que durante todo el proceso, lo único que se manejan son llaves públicas y privadas, lo que hace del proceso algo completamente anónimo, con la garantía de que no existe una autoridad central que controle o manipule indebidamente la transacción.
- También cabe mencionar que cualquier interesado se puede incorporar a la red de validación sin necesidad de solicitar permismo a ninguna autoridad reguladora y comenzar a recibir remuneración por su trabajo de validación.

Exchanges

- Como no es seguro depositar dinero a un tercero en su cuenta bancaria con la esperanza de que el tercero corresponda con la cantidad de bitcoins acordados, las casas de intercambio funjen como mediadores que garantizan tanto a los compradores como a los vendedores que su acuerdo será llevado a cabo bajo los términos establecidos por ambas partes.
- De la manera anterior, se crea un mercado abierto de “posiciones de compra” y de “posiciones de venta” en el que cada parte publica la cantidad y el precio al que está dispuesto a vender o a comprar un activo. En el instante en que la cryptomoneda alcanza dicho valor, se produce la operación de compra-venta.
- Evidentemente si una posición de compra-venta es muy lejana del precio actual, sería posible que la transaccón NO se llevará a cabo nunca.

Contratos inteligentes

- Un contrato inteligente es un acuerdo electrónico entre dos partes que se ejecuta en el instante en el que se cumplen ciertas condiciones previamente definidas en tal contrato y aceptadas por ambas partes.
- Ejemplo 1: Venderé 5.32 Bitcoins en el momento en el que cualquier comprador ofrezca pagarlos a un valor de 42,730 dólares por cada uno de ellos. (Sell Limit)
- Ejemplo 2: Compraré 3.21 Etherum en el momento en el que cualquier vendedor ofrezca venderlos a un valor de 3500 dólares cada uno. (Buy Limit)
- Ejemplo 3: Venderé **a precio de mercado** el total de mi tenencia en bitcoins si el precio cae por debajo de los 41,000 usd por bitcoin (Stop Loss)
- Ejemplo 4: Venderé **a precio de mercado** el 50% de mi tenencia si el precio supera los 51,000 usd. (Stop Limit)

GRACIAS !!!

Gustavo Arellano

Twitter: @arellano_gus