**Objetivo:**

1. Exchange de criptos (trading).
   1. Exchange centralizado: el 99% de operaciones actualmente se realizan por exchanges centralizados por varios motivos (i) la gente no sabe realmente su peligro (ii) la gente no sabe que existen descentralizados (“existen”) (iii) el uso de los descentralizados es difícil y poco amigable. En resumen, ellos poseen tus claves privadas, el order book lo tienen en un servidor centralizado y a menudo parece que tienen problema de liquidez y withdraw. Tienen el problema del front-running.
   2. Exchanges descentralizados: hay muchos intentos de soluciones. Hacen uso de ATOMIC SWAPS y de HashTimeLockContracts (HTLC). Sin embargo, por temas de eficiencia parece que muchos de ellos pese a dejar que el usuario gestione sus claves privadas, el order book lo tienen en un servidor centralizado. Tienen el problema del front-running.
2. Bolsa. En el caso de la bolsa el Order Book está centralizado. También se encuentra centralizada su ubicación, es por esto que existe el HFT (?). Pensar qué se podría hacer aquí o en exchanges descentralizados (con el orderbook descentralizado también).

**ToDo:**

Valorar con Javier antes de dedicarle más tiempo

Corroborar que bolsa/Exchange funciona con un order book al que se lanzan bid/ask para un determinado precio. Antes de entrar al orderbook se observa si hay alguna con la que haga match y se hace automáticamente. ¿Cómo funciona el precio entonces?

Leer más sobre AtomiSwap y HTLC

Leer sobre HFT más

El front-running es lo mimso que el arbitraje?

**Remark:** tener en cuenta que si se tiene un orderbook descentralizado, las ordenes (bid/ask) van a ser publicas también, por lo tanto debido al tiempo de minado de cada tx se abre la posibilidad del front-running…veo que hay una bid/ask que aún no se ha minado y lanzo yo una bid/ask aprovechando lo que se con una fee mayor de manera que se minará antes que la otra operación que sigue en el pool y me aprovecho.

**Opinión personal tras estudiar situación actual:**

Actualmente no hay ninguna solución óptima de ningún tipo (centralizada, semi-descentralizada o descentralizada).

Las soluciones centralizadas son las más utilizadas debido a la rapidez con la que se ejecutan las órdenes. Esto se consigue a costa de que el Exchange posee el activo, las claves o que se realiza un cambio del activo por otro de uso interno. En todos los casos el riesgo de robos es extremo (múltiples casos de robo) ya que el usuario deja de poseer el activo. A su vez se han observado problemas de liquidez e inconvenientes a la hora de retirar fondos. Otro de los grandes problemas asociado a la centralización es el Front-running.

Existen exchanges descentralizados tanto de tokens ERC20 como de criptodivisas. El principal problema es la latencia. En el caso de que los nodos (descentralizados) encargados de los Order Books también ejecuten las ordenes, aparece el Front-running. Al ser transacciones publicas aparece el problema del arbitraje. Si estos nodos solo publican el order book pero son los usuarios los que ejecutan las ordenes (Taker) (i) se complica el proceso de una orden aumentando el tiempo empleado en ella, (ii) otro usuario puede adelantarse poniendo una tx con mayor fee y se desperdiciaría gas (en realidad serían muchos usuarios los que colisionarían (in)voluntariamente, se ha observado en la realidad).

Las soluciones semi-descentralizadas en mi opinión son la futura opción más óptima, ya que debe haber uno o varios puntos de centralización ya sea en el order book o en los nodos encargados del order book. Un pequeño grado de centralización puede ser aceptable, lo que es inadmisible es la posibilidad del front-running o arbitraje. Un timestampeado de cada orden solucionaría la mayoría de los problemas en todos los casos.