Departamento de Ingeniería Sistemas y Computación.

Simulador de envíos cripto y optimización de ordenes para múltiples exchanges

Estudiantes:
Juan Andrés Eslava Tovar
Alejandro José Segura Torres

Asesor:
Valérie Gauthier Umaña

Co-asesor:
Martín Andrade

Proyecto de grado para optar al título de
Ingeniero de Sistemas y Computación

Bogotá D.C., Colombia
10 de junio de 2025

Universidad de los Andes

Índice

Universidad de los Andes

Agradecimientos

Universidad de los Andes

Introducción

La tecnología blockchain ha emergido en el panorama digital contemporáneo como una fuerza transformadora que está cambiando sectores críticos como las finanzas, la logística, la energía y los servicios digitales. Se ha consolidado rápidamente como una tecnología esencial para llevar a cabo trazabilidad de operaciones de manera segura, no falsificable y descentralizada. Creando así un ecosistema en el que la confianza no se deposita en intermediarios centralizados, sino en la robustez de algoritmos criptográficos y en la transparencia del consenso distribuido. Este sistema cambia la forma en que interactuamos con la información al permitir que las transacciones se registren de forma inmutable, auditable y resistente a la manipulación. Al reducir la dependencia de las autoridades centrales, la descentralización fomenta modelos de gestión de datos más democráticos y abiertos a las personas. Además, refuerza la seguridad de la información al eliminar puntos únicos de fallo y garantizar la integridad de los datos mediante mecanismos criptográficos avanzados. En conjunto, blockchain no sólo cambia las infraestructuras tecnológicas, sino que también impulsa un cambio cultural hacia una mayor responsabilidad digital, autonomía y seguridad de la información.

El surgimiento de las criptomonedas marcó uno de los primeros y más visibles usos de la tecnología blockchain. En 2009, Bitcoin fue presentada por un autor anónimo bajo el seudónimo de Satoshi Nakamoto como una forma de dinero digital que no dependiera de bancos centrales ni instituciones financieras para operar, permitiendo transferencias entre pares (peer-to-peer) con un nivel sin precedentes de transparencia y seguridad. Años más tarde, en 2015, Ethereum amplió esta visión al introducir contratos inteligentes, programas autoejecutables que operan sobre la blockchain y permiten automatizar acuerdos sin intermediarios. Estas iniciativas no solo abrieron la puerta a nuevos modelos económicos descentralizados, sino que también encendieron un debate global sobre el papel de los intermediarios tradicionales, el diseño de sistemas económicos más inclusivos y los límites regulatorios en entornos sin autoridad central.

Sin embargo, esta nueva propuesta trae consigo desafíos significativos. Si bien su arquitectura técnica y su promesa de descentralización ofrecen una alternativa poderosa frente a los sistemas tradicionales, también abren la puerta a un conjunto de interrogantes aún no resueltos en los planos jurídico, económico y regulatorio. La creación de criptomonedas y plataformas descentralizadas plantea dilemas sobre el papel futuro de los bancos centrales, la trazabilidad de las operaciones para efectos fiscales y los mecanismos adecuados para garantizar el cumplimiento legal en entornos donde no existen intermediarios tradicionales. A pesar del entusiasmo que rodea a las criptomonedas y el creciente uso de plataformas descentralizadas, muchas personas aún se enfrentan a barreras técnicas considerables. Comprender

las complejidades entre diferentes blockchains, los costos variables de las transacciones, las latencias inherentes a la red y los diversos mecanismos de validación, como Prueba de Trabajo o Prueba de Participación, puede resultar un terreno complicado. Estos elementos, lejos de ser meros detalles técnicos, son cruciales a la hora de gestionar activos digitales o ejecutar órdenes de compra y venta, especialmente para organizaciones que manejan grandes volúmenes de capital y buscan optimizar cada operación.

Aqui debería ir hablado lo que hicimos con el optimi En este contexto, el objetivo de esta tesis es permitir la simulación y comparación de transacciones en el ecosistema de criptomonedas, con el objetivo de optimizar tanto los costos involucrados como el rendimiento general de las operaciones.

El proyecto contempla un análisis comparativo de los envíos de activos digitales entre billeteras conectadas a diferentes blockchains, con el objetivo de explorar rutas y puentes (bridges) que permitan identificar las opciones más eficientes en términos de costo y latencia. Asimismo, se desarrollaron estrategias para la optimización de órdenes de compra y venta en exchanges, enfocadas en minimizar el impacto del slippage (deslizamiento de precios) y maximizar la eficacia de las transacciones mediante una distribución inteligente del capital disponible.

El desarrollo de este trabajo se estructura en tres capítulos principales que permiten abordar de forma progresiva y ordenada los elementos teóricos, metodológicos y analíticos necesarios para la construcción y evaluación del modelo propuesto.

En el Capítulo 1 se expone el marco teórico fundamental para comprender el funcionamiento del ecosistema blockchain. Se describen los principios técnicos esenciales que sustentan esta tecnología, tales como sus principales tipologías, los mecanismos de consenso utilizados en la validación de transacciones, entre ellos la Prueba de Trabajo (PoW) y la Prueba de Participación (PoS), así como el funcionamiento de las billeteras digitales. Este apartado tiene como finalidad proporcionar una base conceptual sólida que permita contextualizar los análisis posteriores, facilitando la comprensión del comportamiento de las criptomonedas y del manejo técnico requerido para el diseño y ejecución de simulaciones en entornos descentralizados.

El Capítulo 2 se centra en el diseño metodológico del estudio, con énfasis en la identificación de los factores que inciden en la eficiencia de las transacciones con criptoactivos. En primer lugar, se analizan variables críticas como la latencia de red, los costos de transacción (gas fees) y la profundidad de mercado en plataformas de intercambio (exchanges). A partir de este análisis, se desarrolla un modelo de simulación que permite determinar rutas óptimas para la transferencia de activos entre billeteras digitales, integrando información en tiempo

real proveniente de diversas APIs y servicios de puentes entre cadenas (bridges). Asimismo, se proponen y evalúan estrategias para la ejecución de órdenes de compra y venta que buscan minimizar el slippage y optimizar el uso del capital disponible.

Finalmente, en el Capítulo 3 se presentan los resultados obtenidos tras la implementación del modelo, así como la discusión correspondiente y las conclusiones del estudio. Este apartado permite valorar la efectividad de las estrategias propuestas y delimitar posibles líneas futuras de investigación.

Como acabe el optimizador tambien ponerlo en el cap 2 y en dado caso buscar la grabacion minuto 31 Aqui poner una introduccion de como hicimos el optimi, y saber vender este producto en este caso el optimi

La estructura de esta tesis combina una rigurosa investigación teórica con un análisis técnico detallado, el desarrollo práctico utilizando Python y la integración con herramientas fundamentales del ecosistema Web3. A lo largo de los siguientes capítulos, el lector encontrará una guía clara y progresiva que abarca desde los conceptos fundamentales que sustentan el sistema propuesto hasta la presentación de simulaciones concretas y proyecciones sobre su escalabilidad y aplicabilidad en escenarios reales.

En definitiva, esta investigación no solo busca responder a un reto técnico de actualidad, sino que también aspira a aportar conocimiento útil y accionable en un momento crucial, donde la adopción masiva de tecnologías descentralizadas se perfila como una realidad cada vez más cercana.

Universidad de los Andes

Capítulo 1: Fundamentos de blockchain y criptoactivos

Este capítulo presenta los fundamentos conceptuales y técnicos necesarios para comprender el desarrollo de un optimizador de transacciones cripto aplicado al caso de la empresa Peccala. Se abordan temas relacionados con blockchain, billeteras, exchanges, costos, latencia, seguridad, mecanismos de consenso y modelos de trading, los cuales sirven como base para el diseño del sistema propuesto.

Principios Técnicos y Funcionales de la Tecnología Blockchain

La tecnología blockchain, en su esencia, puede describirse como un libro de contabilidad digital distribuido y cronológico. Este libro está compuesto por una cadena de bloques de información, donde cada bloque contiene un conjunto de registros o transacciones. Una vez que un bloque se añade a la cadena, su contenido se vuelve extremadamente difícil de alterar, lo que proporciona una base sólida para la confianza y la transparencia en las interacciones digitales.

Lo que hace a la blockchain verdaderamente disruptiva es su capacidad para operar sin una entidad central que controle o valide las transacciones. En lugar de depender de un intermediario, como un banco o una autoridad central, la validación y el mantenimiento de la integridad de la cadena son tareas que realizan de forma colectiva y coordinada los participantes de la red, conocidos como nodos. Estos nodos alcanzan un consenso sobre la validez de las transacciones y el estado actual de la cadena mediante algoritmos de consenso.

1. **Blockchain: Más que una Base de Datos Distribuida** Aunque a menudo se describe como una "base de datos distribuida", esta definición, aunque correcta, no abarca todas las características únicas de la blockchain. Esta tecnología es un tipo específico de base de datos distribuida que posee propiedades singulares:

    - **Estructura en Bloques Encadenados:** En la blockchain, los datos, que pueden incluir transacciones o información, se agrupan en "bloques". Cada bloque, además de contener los datos, incluye una referencia criptográfica al bloque anterior, conocida como su "hash", junto con una marca de tiempo. Este encadenamiento de bloques mediante hashes es fundamental para la seguridad y la inmutabilidad de la cadena. Un nuevo bloque solo puede añadirse a la cadena si ha sido validado por la red y hace referencia correctamente al bloque que lo precede.
    - **Consenso Distribuido:** Para añadir un nuevo bloque a la cadena, los nodos de la red deben alcanzar un acuerdo sobre su validez, conocido como consenso. Existen

diferentes algoritmos de consenso, como la Prueba de Trabajo (Proof of Work) y la Prueba de Participación (Proof of Stake), cada uno con sus propias reglas, ventajas y desventajas en términos de seguridad, eficiencia energética y descentralización. Este proceso de consenso garantiza que todos los nodos mantengan una copia idéntica y actualizada de la blockchain, lo que refuerza su integridad.

2. **Características Principales de la Tecnología Blockchain**

Las siguientes características son intrínsecas al diseño de la mayoría de las blockchains y son la base de su propuesta de valor:

a) **Descentralización:** La descentralización en blockchain implica la ausencia de un único punto de control o fallo. En lugar de que los datos y la autoridad estén centralizados en un servidor o entidad, la información se replica y distribuye entre múltiples nodos en una red peer-to-peer (P2P). Las decisiones, como la validación de transacciones, son distribuidas y gestionadas a través de mecanismos de consenso.

   Esta arquitectura incrementa la resiliencia del sistema; si algunos nodos fallan, la red sigue operando. Además, reduce la dependencia de intermediarios, lo que disminuye costos y posibles censuras. Sin embargo, es importante señalar que el grado de descentralización puede variar significativamente entre diferentes blockchains.

b) **Inmutabilidad (o Resistencia a la Manipulación):** Una vez que una transacción ha sido validada y añadida a la cadena, se vuelve extremadamente difícil de modificar o eliminar. Esto no implica que sea completamente imposible, pero desde una perspectiva computacional y económica, resulta inviables en blockchains bien establecidas. Alterar un bloque anterior requeriría recalcular el hash de ese bloque y de todos los bloques subsiguientes, así como obtener el consenso de la mayoría de la red, lo que representa una tarea monumental.

   La inmutabilidad se logra a través del encadenamiento criptográfico de los bloques y de los mecanismos de consenso. Esta característica garantiza la integridad y la auditabilidad de los registros, creando un historial confiable y permanente.

c) **Seguridad criptográfica:** La seguridad en blockchain se basa en técnicas criptográficas avanzadas. Dos de los elementos fundamentales son:

   - **Funciones Hash Criptográficas (por ejemplo, SHA-256):** Estas funciones toman una entrada de cualquier tamaño y producen una salida de tamaño fijo (el "hash"). Son deterministas, lo que significa que la misma entrada siempre genera

el mismo hash. También son eficientes, resistentes a la preimagen y a colisiones, y se utilizan para asegurar la integridad de los datos en los bloques y en la generación de direcciones.

- **Firmas Digitales (Criptografía de Clave Pública/Privada):** Cada participante en la red tiene un par de claves: una clave privada, que se mantiene en secreto, y una clave pública, que puede compartirse. Las transacciones se "firmançon la clave privada del emisor, y esta firma se puede verificar utilizando la clave pública correspondiente, garantizando la autenticidad, la integridad y el no repudio de la transacción.

d) **Transparencia (y Pseudonimato):** En las blockchains públicas, como Bitcoin o Ethereum, todas las transacciones y datos de los bloques son visibles para cualquier persona. Cualquier participante puede descargar una copia completa del libro mayor o usar exploradores de bloques en línea para verificar el historial de operaciones. Sin embargo, aunque las transacciones son transparentes, las identidades de los participantes suelen ser pseudónimas. Esto significa que las transacciones se vinculan a direcciones criptográficas, no directamente a identidades del mundo real. Si una dirección se vincula a una identidad, es posible rastrear toda su actividad.

   No todas las blockchains son completamente transparentes. Las blockchains privadas o de consorcio pueden restringir el acceso a un conjunto específico de nodos, ofreciendo mayor privacidad y control para aplicaciones empresariales.

   La transparencia en blockchains públicas fomenta la confianza al permitir auditorías públicas y la verificación independiente de las transacciones. Sin embargo, es crucial encontrar un equilibrio entre la transparencia y la privacidad, ya que diferentes arquitecturas de blockchain abordan esta cuestión de maneras diversas.

En resumen, la tecnología blockchain no solo representa una innovación técnica, sino que está redefiniendo cómo interactuamos y confiamos en el entorno digital. Al comprender sus características fundamentales, podemos apreciar mejor su potencial para transformar diversas industrias y la manera en que manejamos la información y las transacciones.

Clasificación de Infraestructuras Blockchain según Nivel de Acceso y Gobernanza

El diseño y la arquitectura de una solución blockchain no son uniformes; en realidad, varían significativamente según quién puede participar, quién controla la red y cómo se

toman las decisiones. Estos factores determinan el nivel de acceso, el modelo de gobernanza y el grado de descentralización, dando lugar a diferentes configuraciones de infraestructura. Comprender estas diferencias es crucial para seleccionar o diseñar la blockchain adecuada para un propósito específico.

Las infraestructuras blockchain se clasifican principalmente en dos categorías: no permisionadas (abiertas) y permisionadas (restringidas). A continuación, se presenta una descripción clara y accesible de cada tipo.

- **Blockchain Pública (No Permisionada):** Una blockchain pública es una red abierta donde cualquiera puede unirse, leer información, realizar transacciones y participar en la validación de estas mediante el consenso. Este tipo de blockchain se caracteriza por su alta descentralización, transparencia y resistencia a la censura, lo que fomenta la confianza entre los usuarios sin necesidad de intermediarios. Ejemplos icónicos de blockchains públicas son Bitcoin y Ethereum.

  Sin embargo, las blockchains públicas enfrentan desafíos, como la escalabilidad y la eficiencia. Esto puede resultar en velocidades de transacción más lentas y costos transaccionales que, en ocasiones, son altos y variables. Algunas blockchains, especialmente las que utilizan el mecanismo de Prueba de Trabajo (PoW), tienen un considerable consumo energético. Además, el proceso de gobernanza para implementar cambios puede ser lento y complejo, ya que requiere un amplio consenso dentro de la comunidad.

  Casos de Uso Típicos: Criptomonedas, registros públicos inmutables, aplicaciones descentralizadas (dApps) de acceso universal.

- **Blockchain Privada (Permisionada - Entidad Única)** Una blockchain privada es controlada por una sola organización que gestiona los permisos de acceso, las reglas y la validación de las transacciones. Este tipo de blockchain ofrece alta eficiencia, velocidad, privacidad de datos y una gobernanza clara y centralizada. Un buen ejemplo es Hyperledger Fabric, que se despliega para uso interno de una empresa.

  La principal desventaja de una blockchain privada es la significativa reducción o ausencia de descentralización. Esto implica que la confianza se deposita en la entidad administradora, lo que puede generar riesgos en cuanto a un punto único de fallo o control. En este sentido, no es intrínsecamente "trustless", ya que la entidad podría, teóricamente, censurar o manipular información si así lo decide.

  Casos de Uso Típicos: Aplicaciones empresariales internas, como gestión de cadenas de suministro, auditorías internas o manejo de datos confidenciales.

- **Blockchain híbrida:** La blockchain híbrida combina elementos de blockchains públicas y privadas (o de consorcio) para lograr un equilibrio específico entre privacidad, control y transparencia. Su arquitectura es flexible y busca, a menudo, anclar datos de una red permisionada en una pública para mayor seguridad o permitir interacciones controladas. Ejemplos de este tipo incluyen XinFin (XDC Network) y, en ciertos aspectos de su arquitectura, Ripple (XRP Ledger).

  El diseño e implementación de sistemas híbridos pueden ser considerablemente complejos. La gobernanza que rige la interacción entre los componentes públicos y privados requiere una cuidadosa definición. Además, la seguridad general del sistema híbrido depende críticamente de la robustez de cada uno de sus componentes y de la correcta y segura integración entre ellos.

  Casos de Uso Típicos: Aplicaciones que requieren confidencialidad para ciertos datos, pero transparencia o validación pública para otros, como la tokenización de activos o la integración de sistemas financieros tradicionales con el ecosistema descentralizado.

- **Blockchain de Consorcio o Federada (Permisionada - Múltiples Entidades)** Una blockchain de consorcio es gestionada por un grupo de organizaciones preseleccionadas, distribuyendo el control y la validación entre sus miembros. Este tipo de blockchain busca un equilibrio entre la eficiencia de las blockchains privadas y una descentralización controlada, lo que la hace ideal para colaboraciones B2B con intereses compartidos. Ejemplos incluyen Corda de R3 y Energy Web Foundation.

  Sin embargo, la gobernanza entre múltiples organizaciones puede volverse compleja. La coordinación para establecer y mantener acuerdos puede ser un desafío, y existe el riesgo potencial de colusión entre los miembros del consorcio. Además, la configuración inicial y el mantenimiento de esta infraestructura pueden ser más costosos y laboriosos que en una blockchain privada.

  Casos de Uso Típicos: Colaboraciones interempresariales, cadenas de suministro con múltiples actores, liquidaciones interbancarias y registros compartidos sectoriales.

Algoritmos de Consenso y Validación en Redes Distribuidas

Para comprender el funcionamiento de redes distribuidas como las blockchains, es esencial abordar el desafío de lograr que múltiples participantes, sin una autoridad central que los supervise, lleguen a un acuerdo unificado sobre el estado correcto de la red. Este es el propósito de los mecanismos de consenso, que son protocolos y algoritmos fundamentales para validar transacciones, asegurar la inmutabilidad del registro y garantizar la integridad

del sistema, incluso cuando algunos nodos pueden fallar o actuar de manera deshonesta. Validar una transacción implica verificar su autenticidad y legitimidad dentro de las reglas de la red, asegurando, por ejemplo, que no se intente realizar un doble gasto. El mecanismo de consenso garantiza que todos los nodos honestos acuerden qué transacciones son válidas y en qué orden se añaden al registro compartido. Existen diversos mecanismos de consenso, cada uno con sus propias aproximaciones, prioridades y compromisos en cuanto a seguridad, velocidad, escalabilidad y descentralización.

A continuación, se describen algunos de los mecanismos de consenso más relevantes en redes distribuidas, explicados de manera sencilla y accesible. Los más relevantes son [1], [2]:

- **Proof of Work (PoW):** Uno de los mecanismos pioneros, utilizado notablemente por Bitcoin, es el Proof of Work (PoW). La idea central de PoW es que los participantes, conocidos como "mineros", inviertan una gran cantidad de esfuerzo computacional para obtener el derecho a proponer el siguiente bloque de transacciones. Estos mineros compiten resolviendo un complicado acertijo matemático que consume considerable poder de procesamiento y energía. El primer minero en encontrar la solución válida "gana"la oportunidad de publicar el bloque y recibe una recompensa. La seguridad de PoW radica en el elevado costo computacional y energético requerido para producir bloques válidos, lo que hace que modificar el historial sea extremadamente difícil y costoso, siempre y cuando la mayoría de la red sea honesta. Sin embargo, a pesar de su robustez y descentralización, PoW tiene desventajas significativas, como su alto consumo energético, la relativa lentitud en la validación de transacciones y el riesgo de centralización del poder de minado en grandes grupos.

- **Proof of Stake (PoS):** Como alternativa más eficiente energéticamente al mecanismo Proof of Work (PoW), se desarrolló el Proof of Stake (PoS). Este modelo permite a los participantes, conocidos como validadores, verificar transacciones y proponer nuevos bloques en función de la cantidad de criptomonedas que están dispuestos a bloquear como garantía, en un proceso llamado staking.

  Los validadores inmovilizan sus fondos y son seleccionados, generalmente de forma semi-aleatoria y ponderada por el tamaño de su stake, para validar bloques. La seguridad del sistema PoS se basa en incentivos económicos: si un validador actúa de forma deshonesta, puede perder parte o la totalidad de su stake mediante un proceso conocido como slashing. Por el contrario, si cumple su función correctamente, recibe una recompensa.

  Este enfoque no solo reduce significativamente el consumo energético, sino que también permite tiempos de validación más rápidos. Redes como Ethereum (tras su transición

desde PoW), Cardano y Polkadot han adoptado variaciones de este mecanismo. No obstante, el modelo PoS también enfrenta retos, especialmente relacionados con la concentración de poder en manos de grandes tenedores, lo cual exige un diseño cuidadoso para preservar la equidad y la seguridad del sistema.

- **Proof of Staked Authority (PoSA):** El Proof of Staked Authority (PoSA) es una variante híbrida que combina el concepto de stake con un conjunto más limitado y, a menudo, pre-seleccionado o autorizado de validadores. Estos validadores, que deben depositar una garantía (stake), son responsables de la creación de bloques, pero su inclusión en este grupo requiere un proceso de reputación, elección o validación por parte de la comunidad o la entidad emisora. Este diseño permite un rendimiento muy alto y bajos costos de transacción, gracias al número reducido y coordinado de validadores, siendo también eficiente energéticamente. Un ejemplo de red que implementa PoSA es la BNB Chain (anteriormente Binance Smart Chain). Sin embargo, la principal desventaja de PoSA es que sacrifica un grado significativo de descentralización en favor de la velocidad y eficiencia, concentrando el poder de validación en un grupo más pequeño y conocido de entidades.

- **Proof of History (PoH):** A diferencia de los mecanismos anteriores, la Proof of History (PoH) no es un mecanismo de consenso completo por sí mismo, sino un componente diseñado para acelerar y mejorar el proceso de consenso subyacente, comúnmente asociado con PoS. PoH crea un registro histórico verificable del tiempo y el orden de los eventos mediante una función criptográfica secuencial, conocida como una función de retraso verificable (VDF). Esto genera un relojçriptográfico que permite a los nodos contar con una referencia fiable sobre el orden temporal de las transacciones antes de que se complete el consenso final. Al reducir la necesidad de que los nodos intercambien mensajes extensos para acordar el orden de los eventos, PoH simplifica y acelera enormemente el mecanismo de consenso principal con el que se combina. Solana es la red más conocida que utiliza PoH junto con un mecanismo de PoS (Tower BFT) para lograr su arquitectura de alto rendimiento.

En conclusión, la selección de un mecanismo de consenso es una decisión arquitectónica crucial para cualquier red distribuida, ya que define su equilibrio entre seguridad, descentralización, velocidad y eficiencia. PoW ofrece una seguridad probada y descentralización, pero a costa de un alto consumo de energía y una velocidad limitada. Por otro lado, PoS mejora la eficiencia y el rendimiento al basarse en incentivos económicos; PoSA prioriza el alto rendimiento y bajos costos, aunque a expensas de la descentralización; y PoH es una técnica

innovadora que acelera los mecanismos de consenso existentes al proporcionar un registro histórico verificable. Comprender estos diferentes enfoques es clave para analizar y comparar las capacidades de las diversas plataformas blockchain y de libro mayor distribuido.

Arquitecturas de Custodia y Gestión de Activos Digitales

La interacción con activos digitales, como criptomonedas y tokens, requiere herramientas especializadas que permiten a los usuarios poseer, enviar y recibir estos activos de manera segura. Estas herramientas se conocen comúnmente como billeteras de activos digitales o "wallets". Es fundamental entender que, a diferencia de una billetera física que guarda dinero, una billetera digital no almacena los activos en sí mismos. En cambio, los activos digitales existen en un registro distribuido (como una blockchain). Lo que una billetera realmente almacena y gestiona son las claves criptográficas necesarias para demostrar la propiedad de esos activos y autorizar transacciones en la red.

Dentro de estas claves, la más crítica es la clave privada. Puedes pensar en ella como una contraseña maestra extremadamente larga y compleja. Esta clave es el secreto que te da control total sobre los activos asociados a una dirección pública, la cual actúa como tu número de cuenta bancaria. Si pierdes tu clave privada o esta cae en manos equivocadas, pierdes el control de tus activos. Por lo tanto, la seguridad y gestión de esta clave privada son el núcleo de la tecnología de billeteras. Las billeteras varían significativamente en cómo gestionan estas claves, lo que lleva a diferentes tipos y arquitecturas. Las clasificaciones más importantes se basan en su conexión a internet y en quién custodia la clave privada.

Clasificación por conexión a internet

Una forma común de clasificar las billeteras es por su conexión a internet:

- **Billeteras calientes (Hot Wallets):** Estas billeteras están siempre en línea o se conectan a internet regularmente para funcionar. Generalmente, se presentan como software que se ejecuta en un ordenador (como aplicaciones de escritorio), en un teléfono móvil (aplicaciones móviles) o como extensiones en navegadores web. La clave privada se almacena digitalmente en el dispositivo o servicio conectado a internet. Su principal ventaja es la conveniencia y la velocidad, permitiendo enviar y recibir transacciones de forma rápida y sencilla. Ejemplos populares incluyen MetaMask y Trust Wallet. Sin embargo, al estar conectadas a internet, son inherentemente más susceptibles a ataques en línea, como hackeos, malware o intentos de phishing, ya que la clave privada reside en un entorno potencialmente expuesto. Por esta razón, son más adecuadas para gestionar pequeñas cantidades de activos que se utilizan para transacciones frecuentes.

- **Frías (Cold Wallets):** Estas billeteras se mantienen desconectadas de internet la mayor parte del tiempo, lo que las convierte en la opción más segura para almacenar activos digitales. La clave privada se guarda en un entorno físico aislado, lejos de cualquier conexión de red. Las formas más comunes de billeteras frías son las billeteras de hardware (dispositivos físicos diseñados específicamente para almacenar claves) y, aunque menos recomendadas por su fragilidad, las billeteras de papel (que simplemente tienen la clave impresa). Para realizar una transacción con una billetera fría, se prepara la transacción en un dispositivo conectado, se transfiere a la billetera fría (por ejemplo, vía USB o código QR), se firma con la clave privada sin que esta salga del dispositivo offline, y luego la transacción firmada se envía de vuelta al dispositivo online para ser emitida a la red. Su principal beneficio es la alta seguridad contra amenazas en línea, siendo ideales para almacenar grandes cantidades de activos a largo plazo. Sin embargo, su desventaja es que son menos prácticas y más lentas para realizar transacciones frecuentes. Ejemplos destacados de billeteras de hardware son Ledger y Trezor.

Clasificación por custodia de la clave privada

Esta clasificación es quizás la más crucial, ya que define quién tiene el control último sobre los activos:

- **Billeteras No Custodiadas (Non-Custodial Wallets):** En este tipo de billeteras, el usuario tiene el control total y exclusivo de su clave privada o de la "frase semilla"(seed phrase), que permite regenerar la clave privada. La billetera, ya sea software o hardware, genera la clave privada en el dispositivo del usuario y esta nunca es compartida con un tercero. El usuario es el único responsable de la seguridad y respaldo de su clave privada o frase semilla. Si la pierde o la olvida, no hay una entidad central que pueda ayudar a recuperarla, y los activos se pierden irremediablemente. Este modelo encapsula el espíritu de la descentralización, ya que el usuario no necesita confiar en un tercero para custodiar sus fondos. Ejemplos de billeteras no custodiadas incluyen Exodus, MyEtherWallet, así como las billeteras de hardware como Ledger y Trezor, y la mayoría de las billeteras calientes de software, como MetaMask y Trust Wallet.

- **Billeteras custodiadas (Custodial Wallets):** En contraste, en una billetera custodiada, un tercero (generalmente un exchange centralizado o un proveedor de servicios financieros) retiene y gestiona la clave privada en nombre del usuario. Cuando un usuario deposita activos en una billetera custodiada, en realidad está transfiriendo el control de esos activos a la entidad. El usuario no tiene acceso directo a la clave privada subyacente; simplemente tiene un derecho sobre un saldo en la base de datos del custodio. La

principal ventaja de este tipo de billetera es la conveniencia, especialmente para operar en plataformas de intercambio, y la responsabilidad de la seguridad técnica recae en el custodio. Ejemplos típicos son las billeteras proporcionadas por grandes exchanges como Binance y Coinbase. Sin embargo, la desventaja fundamental es la pérdida de control: el usuario debe confiar completamente en la seguridad, solvencia y políticas del tercero. Si el custodio es hackeado, quiebra o decide congelar fondos (por razones regulatorias, por ejemplo), el usuario puede perder el acceso a sus activos. El dicho "Not your keys, not your coin"(Si no son tus claves, no son tus monedas) resume el riesgo inherente a la custodia por terceros.

Es importante notar que las clasificaciones a menudo se solapan: una billetera puede ser No Custodiada y Caliente (como MetaMask), No Custodiada y Fría (como Ledger), o Custodiada y Caliente (la interfaz web de un exchange). La elección entre estos tipos de billeteras depende de las necesidades del usuario, el volumen de activos a gestionar, la frecuencia de las transacciones y, crucialmente, su nivel de comodidad con la responsabilidad de la seguridad y la confianza en terceros.

En resumen, comprender la naturaleza y las características de las billeteras criptográficas es vital para cualquier persona que desee interactuar con el mundo de los activos digitales. La elección de una billetera adecuada debe basarse en un equilibrio entre seguridad, conveniencia y el nivel de control que el usuario está dispuesto a asumir. Con el conocimiento adecuado, los usuarios pueden tomar decisiones informadas y proteger sus activos en un entorno digital cada vez más complejo.

Plataformas de Intercambio Cripto: Modelos Operativos y Descentralización

Para que los usuarios puedan adquirir, vender o intercambiar criptoactivos como Bitcoin, Ether y otros tokens, existen plataformas especializadas conocidas como plataformas de intercambio criptográfico o .^{ex}changes". Estas plataformas actúan fundamentalmente como intermediarios que conectan a compradores y vendedores, facilitando las transacciones en un entorno digital. La forma en que operan y, crucialmente, cómo manejan la custodia de los activos de los usuarios, define su arquitectura y se convierte en una distinción clave en el ecosistema cripto. La clasificación principal de los exchanges se basa en su grado de centralización.

a) **Exchanges Centralizados (CEX - Centralized Exchanges)** Los exchanges centralizados operan de manera similar a las bolsas de valores tradicionales, siendo gestio-

nados por una única entidad o empresa. Cuando un usuario desea operar en un CEX, generalmente debe depositar sus criptoactivos (o moneda fiduciaria) en una billetera controlada por el exchange. En este modelo, el exchange custodia las claves privadas de los fondos de los usuarios mientras estos permanecen en la plataforma. Las operaciones de compra y venta se registran en un "libro de órdenesïnterno que mantiene el exchange, y las transacciones se ejecutan rápidamente dentro de sus propios sistemas, fuera de la blockchain. La liquidación en la blockchain solo ocurre cuando un usuario deposita o retira fondos.

Las ventajas principales de los exchanges centralizados son su alta liquidez, lo que permite comprar o vender activos con facilidad, y la velocidad de ejecución de las transacciones, que son rápidas gracias a la infraestructura interna del exchange. Además, suelen contar con interfaces de usuario amigables y ofrecen servicios adicionales como trading de margen, futuros, o incluso funciones de staking y préstamos. Muchos CEX también actúan como puertas de entrada para convertir moneda fiduciaria (como USD o EUR) en criptoactivos. Ejemplos prominentes de CEXs incluyen Binance, KuCoin y Kraken.

Sin embargo, la principal desventaja y riesgo de los CEXs radica en que el usuario cede la custodia de sus claves privadas a un tercero. Esto implica un acto de confianza, ya que el usuario debe confiar en que el exchange protegerá sus fondos de hackeos, no actuará de manera fraudulenta y permitirá retiros cuando sea necesario. La frase "Not your keys, not your coin"("Si no son tus claves, no son tus monedas") resume este riesgo: si el exchange sufre un hackeo mayor o quiebra, los usuarios pueden perder sus activos. Además, al ser entidades centralizadas, están sujetas a regulaciones, lo que a menudo implica requisitos de KYC (Know Your Customer - Conoce a tu Cliente), donde los usuarios deben verificar su identidad, lo que puede ser una barrera para la privacidad o el acceso.

b) **Exchanges Descentralizados (DEX - Decentralized Exchanges)** En contraste, los exchanges descentralizados permiten a los usuarios intercambiar criptoactivos directamente entre sí (peer-to-peer) sin la necesidad de un intermediario que custodie los fondos. Los usuarios operan directamente desde sus billeteras no custodiadas, manteniendo el control total de sus claves privadas. Las transacciones se ejecutan mediante contratos inteligentes (smart contracts) en la blockchain, lo que garantiza la transparencia y elimina la necesidad de confiar en una entidad central.

   Existen diferentes modelos de DEXs: algunos utilizan libros de órdenes que operan total o parcialmente en la blockchain (por ejemplo, Bisq y Hodl Hodl, que a menudo se

enfocan en fiat-to-crypto utilizando mecanismos como multifirma), mientras que otros, muy populares hoy en día, se basan en el modelo de Automated Market Maker (AMM - Creador de Mercado Automatizado). Los AMMs utilizan "pools de liquidez"(fondos de criptoactivos aportados por usuarios que son recompensados) y algoritmos para determinar automáticamente los precios de intercambio, permitiendo a los usuarios "swappear"(intercambiar) tokens directamente con el pool a través de contratos inteligentes (por ejemplo, Uniswap, SushiSwap y PancakeSwap).

Las ventajas clave de los DEXs incluyen que el usuario mantiene el control total de sus claves privadas en todo momento, lo que reduce significativamente el riesgo de pérdida por hackeos del exchange o censura. Generalmente, no requieren KYC, lo que ofrece mayor privacidad y accesibilidad global, y son resistentes a puntos únicos de fallo centralizados. Sin embargo, los DEXs a menudo presentan menor liquidez en comparación con los CEXs (especialmente para pares de activos menos populares), lo que puede resultar en un mayor deslizamiento de precios para operaciones grandes. La velocidad y el costo de las transacciones dependen de la blockchain subyacente y sus tarifas de red ("gas fees"). Las interfaces de usuario pueden ser menos intuitivas para principiantes, y existen riesgos técnicos como vulnerabilidades en los contratos inteligentes o el riesgo de "pérdida impermanente"para los proveedores de liquidez en AMMs.

c) **Modelos Híbridos y Características Integradas** El panorama de los exchanges está evolucionando, y el límite entre CEX y DEX a veces se difumina con la aparición de modelos que intentan combinar lo mejor de ambos mundos o con billeteras no custodiadas que integran funcionalidades de intercambio. Si bien no existe una categoría "Híbrida"única y universalmente definida al mismo nivel que CEX vs. DEX, podemos observar varias aproximaciones:

- **Wallets con Funcionalidad de Swap:** Algunas billeteras no custodiadas (como Coinbase Wallet o Edge Wallet) no son exchanges en sí mismas, pero integran la capacidad de realizar intercambios de activos. A menudo, lo hacen conectándose a protocolos DEX en segundo plano o incluso interactuando con APIs de exchanges centralizados, pero la característica clave es que el usuario mantiene la custodia de sus claves.
- **Exchanges con Componentes Híbridos:** Algunas plataformas buscan optimizar el rendimiento combinando un libro de órdenes off-chain para el emparejamiento rápido de operaciones con liquidación on-chain final para garantizar la

transparencia y la no custodia de los fondos en el momento del intercambio final. Estos modelos buscan la velocidad de un CEX sin sacrificar completamente el control de fondos durante el trading. Ejemplos notables en este espacio, aunque a menudo se clasifican como DEX de Capa 2, incluyen plataformas como dYdX o protocolos como Loopring.

Más allá de la custodia, los exchanges también se diferencian en aspectos operativos clave: las comisiones por transacción (que pueden ser un porcentaje del valor operado o tarifas fijas), la profundidad de mercado (la cantidad de órdenes de compra y venta disponibles a diferentes precios, lo que afecta la facilidad de ejecutar grandes operaciones), la velocidad de ejecución de las órdenes y, como se mencionó, los requisitos de KYC y otras regulaciones que impactan la accesibilidad y la privacidad.

En resumen, la elección entre un exchange centralizado o descentralizado, o una plataforma con características híbridas, implica sopesar la conveniencia, la liquidez y la facilidad de uso (a menudo mayores en CEXs) frente al control total de los activos, la privacidad y la resistencia a la censura (características clave de los DEXs). Comprender estos modelos operativos y sus implicaciones es fundamental para navegar el ecosistema de los activos digitales y tomar decisiones informadas sobre dónde y cómo interactuar con ellos.

Universidad de los Andes

Capítulo 2

Análisis de Latencia Transaccional y Estructura de Costos en Blockchain

En el análisis de redes blockchain, tanto desde la perspectiva del usuario como del desarrollador, el rendimiento suele evaluarse principalmente mediante dos indicadores: la latencia (el tiempo que tarda una transacción en confirmarse) y el costo asociado a dicha transacción. Ambos factores son fundamentales para determinar la usabilidad de la red, su eficiencia, y su capacidad para soportar aplicaciones en diferentes contextos.

a) Latencia transaccional

La latencia hace referencia al tiempo que transcurre desde que una transacción es enviada a la red hasta que se considera confirmada y segura. En la mayoría de las blockchains, una transacción no se considera completamente finalizada con solo aparecer en el siguiente bloque. Para garantizar su seguridad y evitar posibles reversiones, se suele esperar a que se añadan varios bloques posteriores.

Este tiempo puede variar por diversas razones:

- **Congestión de la red:** Cuando el volumen de transacciones supera la capacidad de procesamiento de los bloques, se forma una cola de espera. Los validadores o mineros priorizan aquellas operaciones con tarifas más altas, lo que puede aumentar significativamente la espera de las transacciones que ofrecen comisiones más bajas.
- **Tarifas de transacción (gas fees):** En muchas blockchains, especialmente aquellas que permiten contratos inteligentes, los usuarios pagan una tarifa por incluir sus operaciones en los bloques. Esta tarifa actúa como una especie de subasta: quien paga más, suele ser procesado más rápido.
- **Tipo de red y mecanismo de consenso:** El sistema de consenso influye directamente en la frecuencia con que se generan nuevos bloques. En redes como Bitcoin (Proof of Work), este tiempo puede rondar los 10 minutos. En cambio, blockchains que usan Proof of Stake o modelos híbridos suelen tener tiempos de bloque más cortos, reduciendo así la latencia.
- **Complejidad de la operación:** Las transacciones simples, como transferencias de fondos, se procesan rápidamente. Sin embargo, las que implican contratos inte-

ligentes pueden requerir más recursos y validaciones adicionales, lo cual también puede afectar el tiempo de confirmación.

b) Costos de transacción

El costo de una transacción se refiere a la comisión que debe pagar el usuario para que su operación sea procesada, validada y añadida a la cadena. Este pago incentiva a los validadores o mineros a participar activamente en la red.

Existen distintos elementos que inciden en este costo:

- **Estructura de tarifas de la blockchain:** Cada red define un modelo específico de cobro. En el caso de Ethereum, por ejemplo, cada operación consume una cantidad determinada de "gas", y el precio del gas puede variar según la demanda.
- **Nivel de congestión:** En momentos de alta demanda, las tarifas aumentan porque los usuarios compiten por espacio en los bloques.
- **Tipo y complejidad de la transacción:** Algunas operaciones, como la ejecución de contratos inteligentes complejos, requieren más recursos que una transferencia común, lo que se traduce en un mayor costo.
- **Mecanismo de consenso:** Aunque no siempre es el principal factor, el tipo de consenso también influye. Las redes con alto consumo energético, como las basadas en Proof of Work, tienden a tener costos base más elevados.

A continuación, se muestra una tabla con estimaciones aproximadas de tarifas promedio en distintas redes blockchain, junto con su mecanismo de consenso:

Blockchain	Costo Promedio	Tipo de Consenso
Bitcoin	\$2 - \$10+	Proof of Work (PoW)
Ethereum	\$1 - \$50	Proof of Stake (PoS)
Solana	¡\$0.01	Proof of History + PoS
Binance Smart Chain	\$0.10 - \$0.50	Proof of Staked Authority (PoSA)
Lightning Network	¡\$0.01	Segunda capa sobre BTC

Tabla 1: Comparación de costos de transacción por blockchain

c) Escalabilidad y soluciones de segunda capa

Para reducir los problemas asociados a la latencia y el costo en las redes blockchain base (Layer 1), se han desarrollado soluciones de segunda capa (Layer 2). Estas operan

sobre la cadena principal, procesando transacciones fuera de ella y consolidando los resultados en la red base. Esto permite aumentar la capacidad sin comprometer la seguridad.

Un ejemplo notable es la Lightning Network, una solución diseñada para Bitcoin. Esta red permite realizar micropagos casi instantáneos y con tarifas muy bajas, ideal para transacciones frecuentes entre partes conocidas, sin necesidad de registrar cada una individualmente en la blockchain principal.

Tanto la latencia como el costo de las transacciones son aspectos centrales en la evaluación de cualquier red blockchain. Estos factores no sólo influyen en la experiencia del usuario, sino también en la viabilidad técnica y económica de diferentes casos de uso. La adopción de mecanismos de consenso más eficientes y de soluciones de escalabilidad como las redes de segunda capa puede marcar una diferencia significativa en el rendimiento general de una blockchain.

Impacto de la Profundidad de Mercado y el Slippage en la Ejecución de Órdenes

En el contexto del trading de activos digitales, ejecutar una orden de compra o venta de forma eficiente no depende únicamente de elegir el precio o el momento adecuados. También es crucial considerar las condiciones específicas del mercado en el que se realiza la operación. En particular, dos conceptos resultan fundamentales para entender la calidad de la ejecución: la liquidez y la profundidad del mercado. Cuando estos son insuficientes, se produce un fenómeno conocido como *slippage* o deslizamiento.

¿Cómo se genera el slippage?

Para comprender qué es el slippage, es necesario entender primero cómo operan la mayoría de las plataformas de intercambio —en especial los exchanges centralizados y algunos descentralizados que funcionan con libros de órdenes. Estas plataformas mantienen un order book donde se registran todas las órdenes de compra (también llamadas bids) y de venta (o asks), organizadas por precio. La mejor oferta de compra y la mejor oferta de venta definen el precio de mercado en ese momento.

La liquidez de un activo se refiere a la facilidad con la que puede ser comprado o vendido sin que eso afecte de forma significativa su precio. Un mercado con buena liquidez cuenta con numerosos participantes activos y con un volumen importante de órdenes cerca del precio actual. Por su parte, la profundidad de mercado indica cuánto volumen de compra y venta hay disponible a diferentes niveles de precio, incluso aquellos alejados del valor actual. A

mayor profundidad, mayor capacidad de absorber grandes órdenes sin alterar demasiado el precio.

El slippage ocurre cuando una orden se ejecuta a un precio promedio distinto al que se esperaba inicialmente. Esto suele suceder con las órdenes de mercado, que se ejecutan inmediatamente al mejor precio disponible. Si el volumen de la orden excede el volumen disponible en el primer nivel de precios del libro de órdenes, la orden se empieza a ejecutar en niveles sucesivos, cada vez menos favorables. Esto provoca que el precio promedio final sea peor que el precio que se mostraba al inicio.

Este deslizamiento puede ser especialmente notorio al operar con grandes volúmenes, ya que la orden tiende a consumir buena parte de la liquidez disponible, impactando de forma directa en el precio final. En este contexto, el slippage representa un coste adicional, muchas veces inadvertido, para el trader.

Estrategias para mitigar el slippage

Existen distintas formas de reducir el impacto del slippage, sobre todo cuando se manejan volúmenes altos. A continuación, se detallan algunas de las más relevantes:

- **Análisis de la profundidad del libro de órdenes:** Antes de ejecutar una orden grande, es recomendable revisar cuántas órdenes hay y en qué niveles de precios. Las plataformas de trading suelen ofrecer herramientas visuales que permiten evaluar esta información rápidamente. Si no hay suficiente volumen cerca del precio actual, conviene considerar otras alternativas de ejecución.

- **Uso del VWAP (Volume Weighted Average Price):** El VWAP es un indicador que muestra el precio promedio ponderado por volumen de un activo durante un periodo determinado. Es utilizado como referencia para evaluar si una orden se ejecutó a un precio competitivo. Muchos algoritmos buscan acercarse lo máximo posible al VWAP al ejecutar órdenes grandes, para evitar generar distorsiones en el mercado.

- **División de órdenes (order splitting o iceberg):** En lugar de enviar una única orden grande, esta puede fraccionarse en múltiples órdenes más pequeñas. Estas se lanzan de forma progresiva o incluso con visibilidad limitada (como en las "órdenes iceberg", donde solo se muestra una parte). Esta técnica reduce el impacto directo sobre el libro de órdenes y puede mejorar el precio promedio de ejecución.

- **Ejecución en múltiples plataformas:** Dado que en el ecosistema de activos digitales la liquidez suele estar fragmentada entre diferentes exchanges, ejecutar una orden simultáneamente en varias plataformas puede permitir acceder a una mayor profundidad

de mercado. Esto reduce el riesgo de slippage y optimiza la ejecución general.

El análisis del slippage es especialmente relevante en el marco del segundo módulo del sistema propuesto en esta tesis, cuyo objetivo es optimizar las operaciones de compra y venta distribuidas. Este módulo puede ejecutar transacciones a través de distintas plataformas, cada una con condiciones particulares de liquidez y profundidad. Por ello, anticipar y minimizar el slippage no solo mejora el rendimiento del sistema, sino que también se vuelve un factor crítico para asegurar una ejecución eficiente de las operaciones.

La implementación de estrategias como el análisis previo de profundidad, el uso de algoritmos de ejecución basados en VWAP, la fragmentación de órdenes o la distribución de operaciones entre distintos exchanges, representa un paso esencial para gestionar de forma inteligente grandes volúmenes de activos digitales y garantizar precios de ejecución más competitivos.

Custodia Institucional y Buenas Prácticas de Seguridad: El Caso Fireblocks

La gestión de activos digitales a gran escala, especialmente en el caso de empresas o instituciones financieras, conlleva desafíos mucho más exigentes que los que enfrenta un usuario individual. A medida que crece la inversión institucional en criptomonedas y otros activos digitales, también aumenta la necesidad de soluciones seguras y eficientes que permitan almacenar, gestionar y transferir estos fondos cumpliendo con criterios de gobernanza, auditoría y escalabilidad. A esto se le conoce como custodia institucional.

El principal reto en este tipo de custodia es la protección de la clave privada. Esta clave es la que permite autorizar transacciones, y su compromiso equivale, en la práctica, a perder el control total sobre los fondos. En los métodos tradicionales de almacenamiento, el riesgo suele concentrarse en un único punto de fallo, es decir, en un único lugar o persona que tiene acceso a la clave completa. Esto representa una vulnerabilidad crítica, especialmente en un entorno donde los ataques informáticos son frecuentes y cada vez más sofisticados.

Para abordar este problema, las soluciones modernas han comenzado a integrar técnicas criptográficas avanzadas. Una de las más importantes es el Cómputo Multipartita, conocido por sus siglas en inglés como MPC (Multi-Party Computation).

¿Qué es el MPC?

El MPC es una tecnología que permite que una operación criptográfica, como la firma de una transacción, sea llevada a cabo entre varias partes diferentes sin que ninguna de ellas tenga acceso completo a la clave privada. En lugar de tener la clave almacenada en un solo

lugar, esta se divide en varias partes o "fracciones" (conocidas como shares), que se guardan por separado. Para firmar una transacción, se requiere que un número mínimo de estas partes colaboren en el proceso. Pero lo más importante es que en ningún momento se reconstruye la clave completa en un solo lugar.

Este enfoque aporta dos beneficios principales:

- **Aumenta la seguridad general:** al no existir una única copia de la clave completa, se elimina el riesgo de que un atacante la robe o un empleado la utilice sin autorización.
- **Facilita la implementación de políticas de control interno:** por ejemplo, se puede exigir la participación de varios responsables dentro de una organización para aprobar una transacción, lo que mejora el control y reduce el riesgo de errores o fraudes.

Un caso real: Fireblocks

Uno de los referentes en el uso de MPC dentro del ámbito de la custodia institucional es Fireblocks. Esta plataforma ha sido adoptada por múltiples actores del ecosistema financiero digital, y su arquitectura está basada precisamente en el uso del MPC para proteger las claves privadas de sus clientes.

Además de ofrecer seguridad criptográfica, Fireblocks permite establecer flujos de trabajo seguros, aplicar políticas de acceso personalizadas y llevar un control detallado de las operaciones. Esto es especialmente útil para fondos de inversión, plataformas de intercambio o empresas que manejan operaciones con gran frecuencia y alto volumen, donde la seguridad no puede comprometer la agilidad operativa. Aunque el sistema propuesto en esta tesis (Peccala) no emplea actualmente la tecnología MPC, es importante mencionar plataformas como Fireblocks porque marcan un estándar en cuanto a seguridad y buenas prácticas en la gestión institucional de activos digitales. Tomarlas como referencia permite pensar en futuros desarrollos del sistema que integren mecanismos similares para aumentar su robustez.[3].

Infraestructura API para Optimización y Ruteo Multicadena

El ecosistema de activos digitales está compuesto por múltiples blockchains independientes, lo que plantea el desafío de la interoperabilidad: la capacidad de transferir activos e intercambiar información entre redes distintas. Esta funcionalidad es esencial en contextos como el trading distribuido, donde los activos no siempre están en una misma blockchain. Para facilitar esta interoperabilidad se utilizan puentes blockchain, que permiten mover activos entre cadenas. Existen múltiples soluciones, y para encontrar las rutas más eficientes se utilizan agregadores y APIs multi-puente, como Li.Fi, que integran diferentes protocolos

como Celer, Across o deBridge, automatizando el proceso y optimizando costes y tiempos de transferencia.

Además, las APIs de exchanges (por ejemplo, Binance o Kraken) son fundamentales para acceder en tiempo real a datos de mercado como precios, liquidez y profundidad del libro de órdenes. Esta información es clave para ejecutar órdenes de compra o venta de forma óptima, minimizando costos como el slippage. En el sistema propuesto en esta tesis, se integran ambos tipos de API: por un lado, para mover activos entre distintas blockchains; y por otro, para analizar condiciones de mercado y decidir dónde y cómo ejecutar cada operación. Esta integración permite un sistema más inteligente, eficiente y adaptado a las condiciones reales del entorno de trading.

Universidad de los Andes

Capítulo 3

Modelo de Optimización Experimental para Distribución de Órdenes en Plataformas Cripto

En entornos de trading de criptoactivos, ejecutar órdenes grandes en un solo exchange puede provocar un deslizamiento considerable y una pérdida de eficiencia en la operación. Frente a este problema, surge la necesidad de distribuir inteligentemente el capital entre múltiples plataformas, aprovechando las diferencias de profundidad de mercado, comisiones y precios disponibles. Este capítulo presenta una versión demo de un optimizador diseñado precisamente para abordar ese desafío: simular y calcular la mejor forma de repartir una orden entre varios exchanges para mejorar el resultado final de la operación, ya sea minimizando el costo en compras o maximizando el ingreso en ventas. La herramienta se construyó utilizando datos reales de mercado y aplica un enfoque numérico para reflejar condiciones operativas concretas.

Para entender cómo funciona esta herramienta, a continuación se describen sus principales componentes: desde la lógica de simulación de órdenes en los libros de compra y venta, hasta el flujo interno de la aplicación y el modelo matemático que permite ejecutar la optimización.

Funcionamiento de los Libros de Órdenes

Antes de ejecutar cualquier estrategia de optimización, es necesario comprender cómo se comportan las órdenes dentro de un exchange. Las plataformas centralizadas operan con un mecanismo conocido como libro de órdenes, que actúa como un registro en tiempo real de todas las ofertas activas de compra y venta para un par de trading determinado (por ejemplo, ETH/USDT).

Este sistema se organiza en dos lados: el de asks (ofertas de venta), donde se listan los precios a los que otros usuarios están dispuestos a vender; y el de bids (ofertas de compra), que muestra los precios que los compradores están dispuestos a pagar. Cuando se ejecuta una orden, esta se enfrenta al lado contrario del libro según su tipo (compra o venta), tomando los mejores precios disponibles hasta alcanzar el volumen deseado.

A continuación, se explica con más detalle cómo se simula este comportamiento dentro del sistema desarrollado, con el fin de que los resultados reflejen fielmente las condiciones reales del mercado, incluyendo aspectos clave como el slippage y la variabilidad de precios por volumen.

a) Operaciones de compra

Cuando un usuario decide comprar un activo por ejemplo, adquirir ETH usando USDT, lo que realmente hace es recorrer el lado de las ofertas de venta del libro (asks), desde el precio más bajo hacia arriba. El sistema toma esas ofertas y va sumando volúmenes hasta cubrir el monto que se quiere invertir.

En la práctica, esto significa que si se quiere comprar una cantidad importante, el precio final no será necesariamente el más bajo del libro, sino un promedio ponderado entre los niveles consumidos. Este fenómeno es lo que se conoce como slippage o deslizamiento, y tiene un impacto directo en el coste total de la operación.

b) Operaciones de venta

En el caso contrario cuando se quiere vender un activo, por ejemplo ETH para recibir USDT, el proceso funciona al revés: se accede al lado de las ofertas de compra del libro (bids). El sistema toma las mejores ofertas disponibles, empezando desde el precio más alto, y se va bajando hasta completar el volumen que el usuario desea vender.

Aquí también se genera slippage, ya que si el volumen es significativo, no todo se ejecutará al mejor precio, sino que se irán consumiendo diferentes niveles del libro, lo que afecta al ingreso total que se puede obtener.

c) Ejemplo ilustrativo

Para entender mejor cómo funciona la ejecución de órdenes en la práctica, veamos un caso sencillo usando un libro de órdenes simulado para el par ETH/USDT:

Asks (venta)	**Bids (compra)**
2560.00 — 0.5 ETH	2555.00 — 1.2 ETH
2562.00 — 1.0 ETH	2550.00 — 2.0 ETH

Tabla 2: Ejemplo simplificado de un libro de órdenes para ETH/USDT.

Supongamos que un usuario quiere comprar 1 ETH. El sistema comenzará por tomar los asks más bajos, es decir, los 0.5 ETH ofrecidos a 2560.00. Como aún falta por completar la orden, tomará también 0.5 ETH del siguiente nivel, a 2562.00. El resultado será un precio promedio entre ambas, ligeramente superior al mínimo visible en el libro.

Por otro lado, si se quiere vender 1 ETH, el sistema accederá al lado bid, vendiendo primero 1.0 ETH a 2555.00. Si el volumen fuera mayor, seguiría al siguiente nivel de

precio, bajando progresivamente. Este comportamiento se replica dentro del simulador, permitiendo obtener un resultado lo más cercano posible a una ejecución real.

d) Aplicación en el simulador

Para replicar el comportamiento real del mercado, el simulador implementa una lógica que selecciona el lado correspondiente del libro de órdenes en función del tipo de operación que se desea ejecutar. En concreto, se usa la siguiente estructura condicional en el código:

```
book_side = order_book["asks"] if operation_type == "buy" else order_book["bids"]
```

Esto garantiza que:

- Si se trata de una compra, el sistema recorra las mejores ofertas de venta disponibles.
- Si es una venta, se aprovechen los precios más altos del lado de compra.

Este enfoque permite que la simulación refleje con bastante precisión el efecto que tiene el volumen sobre el precio final incluyendo el slippage, así como las condiciones propias de cada exchange. Al incorporar esta lógica directamente sobre los libros de órdenes obtenidos en tiempo real, el sistema reproduce con fidelidad la experiencia de trading que tendría un usuario en una plataforma real.

Universidad de los Andes

Diagrama de Flujo de la Aplicación

La aplicación desarrollada está diseñada para tomar decisiones automáticas sobre cómo distribuir una orden entre diferentes exchanges. Para lograrlo, sigue una secuencia de pasos bien definida que se resume en el siguiente diagrama de flujo:

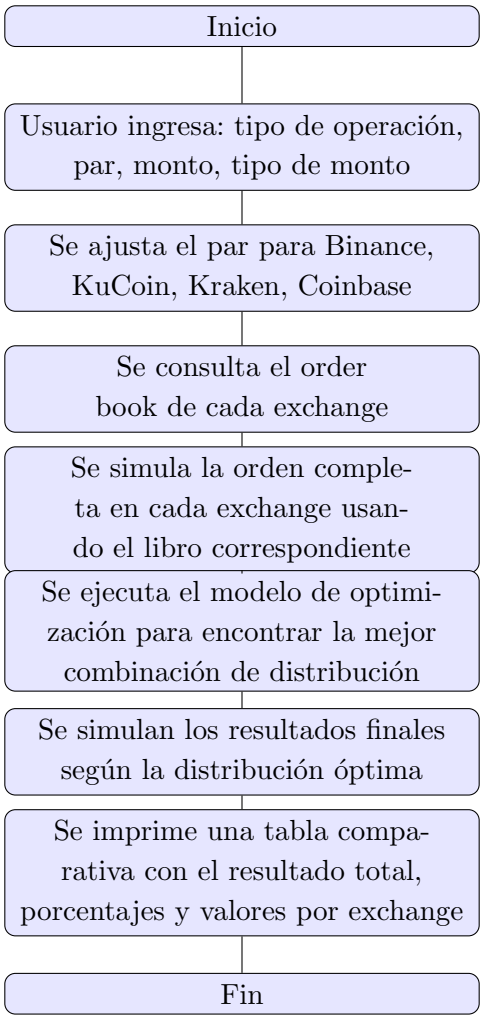

Figura 1: Diagrama de flujo de la aplicación de simulación y optimización de órdenes.

A grandes rasgos, el proceso inicia con la entrada del usuario, quien define el tipo de operación (compra o venta), el par de criptoactivos, el monto a operar y cómo se interpreta ese monto (por ejemplo, si se refiere al activo base o al quote).

Luego, se ajusta el formato del par según el exchange: algunos requieren guiones (como KuCoin), mientras que otros no (como Binance). Una vez configurado, se realiza la consulta

a los libros de órdenes de cada plataforma y se simula la ejecución completa de la orden en cada una, por separado.

A continuación, entra en juego el optimizador, que calcula la mejor forma de repartir el monto total entre los exchanges disponibles. Con esa distribución óptima en mano, el sistema vuelve a simular la operación —esta vez con la división calculada— y presenta los resultados finales en una tabla comparativa. Esta incluye tanto los valores individuales por exchange como el resultado total de la operación.

Modelo Matemático de Optimización

El corazón de esta aplicación es un modelo matemático que determina cómo repartir una orden entre varios exchanges de forma eficiente. La lógica es sencilla en concepto, pero poderosa en resultados: dependiendo del tipo de operación (compra o venta), el modelo decide qué porcentaje del total asignar a cada exchange para lograr el mejor resultado posible.

En términos generales:

- Si se trata de una compra, el objetivo es minimizar el costo total.
- Si es una venta, se busca maximizar el ingreso neto.

Esta optimización se basa en datos reales del mercado, incluyendo slippage y comisiones, lo que hace que el resultado refleje condiciones operativas concretas.

a) Objetivo del modelo

El objetivo principal del modelo depende directamente del tipo de operación que se quiera realizar:

- En una orden de compra, se parte de un monto total en la moneda quote (por ejemplo, USDT) y se intenta obtener la mayor cantidad posible del activo deseado (por ejemplo, ETH). En este caso, el modelo busca minimizar el gasto total requerido para completar la operación, considerando tanto el precio como la comisión en cada exchange.
- En una orden de venta, ocurre lo contrario: se tiene una cantidad fija del activo base (por ejemplo, 2.8 ETH) y se quiere maximizar el ingreso total en moneda quote (por ejemplo, USDT). Aquí, el modelo busca la combinación de distribución que genere la mayor ganancia neta posible.

Ambos casos se resuelven usando una misma estructura matemática, pero adaptando la función objetivo según el contexto. Esta flexibilidad permite que el optimizador se ajuste automáticamente sin necesidad de cambiar su lógica interna cada vez que varía el tipo de operación.

b) Variables de decisión

Las variables de decisión del modelo representan cómo se reparte la orden entre los distintos exchanges disponibles. Si hay n exchanges, se definen $x_1, x_2, \ldots, x_n$ como las proporciones del monto total que se asignan a cada uno de ellos.

Cada x_i es un valor dentro del intervalo $[0, 1]$, y la suma de todas las proporciones debe ser exactamente igual a 1. Esto garantiza que se distribuya el 100 % del monto sin dejar sobrantes ni asignar más de lo disponible.

Por ejemplo, si $x_1 = 0{,}6$ y $x_2 = 0{,}4$, significa que el 60 % de la orden se ejecutaría en el primer exchange y el 40 % en el segundo. Esta forma de modelar permite al optimizador evaluar combinaciones posibles hasta encontrar la más eficiente para el tipo de operación que se está simulando.

c) Parámetros del modelo

El modelo se apoya en una serie de parámetros que definen tanto el contexto de la operación como las características de cada exchange. Los principales son:

- A: monto total a operar. Dependiendo del tipo de operación, puede estar expresado en la moneda base (por ejemplo, ETH) o en la moneda quote (por ejemplo, USDT).
- $f_i(x_i \cdot A)$: función que representa el resultado neto de ejecutar una fracción $x_i \cdot A$ de la orden en el exchange i. Esta función incluye efectos como el slippage y la comisión aplicable en esa plataforma.

Cada parámetro se calcula usando información en tiempo real obtenida directamente de los libros de órdenes de los exchanges. Esto permite que el modelo trabaje con condiciones realistas y tome decisiones ajustadas al mercado actual.

d) Función objetivo

La función objetivo del modelo varía según el tipo de operación. En ambos casos, el objetivo se construye a partir de las funciones f_i, que representan el resultado de ejecutar una parte de la orden en cada exchange.

Caso 1: Compra

Cuando se realiza una orden de compra, el usuario parte de un monto fijo en la moneda quote (por ejemplo, USDT) y quiere obtener la mayor cantidad posible del activo base. Como el simulador devuelve el costo total de cada fracción de orden, el objetivo del modelo es minimizar ese valor total:

$$\min_{x_1,\ldots,x_n} \sum_{i=1}^{n} f_i(x_i \cdot A)$$

Aquí, $f_i(x_i \cdot A)$ representa el costo de ejecutar la fracción x_i de la orden en el exchange i, incluyendo slippage y comisión.

Caso 2: Venta

En una orden de venta, el objetivo es maximizar el ingreso obtenido por vender una cantidad fija del activo base. Como el optimizador utilizado en la implementación (`scipy.optimize.minimize`) solo permite minimizar funciones, se transforma el problema de maximización en una minimización del negativo:

$$\min_{x_1,\ldots,x_n} -\sum_{i=1}^{n} f_i(x_i \cdot A)$$

Este cambio permite aplicar la misma herramienta de optimización sin alterar el enfoque general del modelo.

e) Restricciones

Para que la solución tenga sentido práctico y sea válida dentro del modelo, se imponen dos restricciones clave:

- **Distribución completa:**

$$\sum_{i=1}^{n} x_i = 1$$

  Esta restricción asegura que el monto total se distribuya por completo entre los exchanges, sin dejar partes sin asignar ni exceder el total disponible.

- **Límites individuales:**

$$0 \leq x_i \leq 1 \quad \forall i \in \{1, \ldots, n\}$$

Esto garantiza que ninguna proporción asignada a un exchange supere el 100 % del monto, ni que se asignen valores negativos, lo cual sería inviable.

Estas restricciones son simples pero suficientes para mantener el modelo dentro de un marco coherente y operativo.

f) Evaluación de la función f_i

A diferencia de una función matemática clásica, la función f_i no está definida de forma analítica. En su lugar, se evalúa mediante una simulación directa basada en el comportamiento real del mercado.

Para cada exchange i, la función $f_i(x_i \cdot A)$ se calcula simulando la ejecución de la fracción x_i del monto total. Esta simulación considera:

- El deslizamiento (*slippage*) causado por el volumen operado.
- El precio medio ponderado por volumen ($VWAP$) derivado del libro de órdenes.
- La comisión de trading aplicada al tipo de orden (normalmente tipo *taker*).

Esta aproximación permite capturar las particularidades de cada plataforma en el momento de operar, dando al modelo una visión más precisa y útil de los costos o beneficios reales asociados a cada decisión.

g) Método de solución: algoritmo SLSQP

El problema de optimización se resuelve utilizando el algoritmo *SLSQP* (Sequential Least Squares Programming), disponible en la función `scipy.optimize.minimize` de la biblioteca SciPy.

Este método es especialmente adecuado para este caso porque:

- Permite minimizar funciones no lineales que no tienen una forma analítica explícita.
- Acepta restricciones tanto de igualdad como de desigualdad.
- Permite establecer cotas inferiores y superiores para cada variable.

Dado que la función f_i se evalúa mediante simulación (y no como una expresión cerrada), el algoritmo SLSQP ofrece la flexibilidad necesaria para explorar diferentes combinaciones de proporciones sin requerir derivadas exactas. Además, el número de variables del modelo es reducido, lo que facilita la convergencia del algoritmo en tiempos razonables.

h) Punto de inicio: distribución uniforme

Para iniciar el proceso de optimización, se parte de una distribución uniforme entre todos los exchanges disponibles. Es decir, si hay n exchanges, el punto de partida se define como:

$$x_1 = x_2 = \cdots = x_n = \frac{1}{n}$$

Esta elección tiene varias ventajas prácticas:

- Elimina cualquier sesgo inicial hacia un exchange en particular.
- Asegura que la condición $\sum x_i = 1$ se cumpla desde el comienzo.
- Mejora la estabilidad numérica y la velocidad de convergencia del algoritmo.

Aunque es posible partir de otros puntos, esta estrategia neutral garantiza que el optimizador explore sin influencias previas, permitiendo evaluar de forma más justa la eficiencia de cada plataforma.

i) Ventajas del modelo

Este modelo ofrece varias ventajas que lo hacen útil y adaptable en escenarios reales de trading con múltiples plataformas:

- **Escalable a más exchanges:** no está limitado a dos plataformas. Se puede extender fácilmente a tres o más, ajustando únicamente los parámetros de entrada.
- **Basado en datos reales:** utiliza libros de órdenes en tiempo real, lo que permite tomar decisiones con base en condiciones actuales del mercado, sin depender de supuestos teóricos.
- **Incluye comisiones y slippage:** a diferencia de modelos simplificados, este considera tanto las comisiones por operación como el impacto del volumen (slippage), lo cual hace que los resultados sean más cercanos a lo que sucedería en una operación real.
- **Funciona para compras y ventas:** el mismo modelo se adapta automáticamente según el tipo de operación, sin necesidad de reestructurar la lógica interna.
- **Resuelve el problema numéricamente:** no requiere fórmulas cerradas ni derivadas analíticas. Esto permite trabajar con funciones complejas o desconocidas, como las que surgen al simular interacciones con libros de órdenes.

En conjunto, estas características hacen que el modelo sea una herramienta flexible y realista, especialmente útil para entornos donde se necesita eficiencia operativa sin perder precisión frente a las condiciones del mercado.

Arquitectura del sistema

El sistema desarrollado permite simular y optimizar la ejecución de órdenes de compra o venta de criptomonedas en distintos exchanges, a partir de datos reales en tiempo real. El objetivo es determinar la mejor forma de distribuir una operación entre múltiples plataformas para maximizar el rendimiento o minimizar el costo total. Esta sección describe la arquitectura modular del sistema, haciendo énfasis en la forma en que se estructuran los datos y se articulan los componentes funcionales.

Diseño modular

El sistema se encuentra dividido en módulos independientes, lo cual permite escalabilidad y facilidad para incluir nuevos exchanges u otras funcionalidades. Los módulos principales son:

- **Módulo de recolección de datos**: se conecta a las APIs públicas de los exchanges para obtener el *order book* en tiempo real.
- **Simulador de órdenes**: dado un libro de órdenes, simula la ejecución de una operación, calculando precio promedio, volumen ejecutado, comisiones y total final.
- **Optimizador**: utilizando programación numérica, determina la distribución óptima del monto total entre los exchanges disponibles.
- **Visualización**: genera representaciones gráficas del resultado para facilitar el análisis comparativo entre escenarios.

Entrada y procesamiento

Los usuarios pueden definir cuatro parámetros clave:

- Tipo de operación: `buy` o `sell`.
- Par de trading: por ejemplo, `ETHUSDT`.
- Cantidad a operar.

- Tipo de cantidad: si se refiere al activo base o al activo cotizado (`base` o `quote`).

A partir de estos parámetros, el sistema formatea los símbolos según los requerimientos de cada exchange y recupera los *order books* con la profundidad necesaria.

Unificación de los libros de órdenes

Una vez obtenidos los libros de órdenes de cada exchange, estos se almacenan en una estructura común para facilitar su procesamiento. Todos los cálculos de simulación y optimización se realizan sobre estos datos locales para garantizar la consistencia de los resultados, evitando discrepancias derivadas de nuevos llamados a la API.

Resultados parciales y comparación

Se ejecuta primero una simulación en la que se evalúa cómo se comportaría la ejecución de la orden si se realizara el 100 % en cada exchange individualmente. Luego, se ejecuta el algoritmo de optimización, que determina la mejor forma de dividir el monto total entre los exchanges disponibles. Los resultados se comparan en una tabla que incluye el precio promedio ponderado, el valor de la comisión (*taker fee*), el total final recibido o pagado, y el porcentaje asignado a cada exchange.

Persistencia y visualización

Además de la salida en consola, el sistema genera gráficas automáticas en formato `.png`, almacenadas en una carpeta de resultados. Estas gráficas incluyen la fecha y hora de ejecución, y muestran tanto la comparación individual por exchange como la distribución óptima calculada.

Simulador de Órdenes

El simulador es una de las piezas clave del sistema, ya que permite estimar con precisión el resultado de ejecutar una orden completa en un solo exchange, utilizando el libro de órdenes real obtenido en tiempo real. Esta simulación tiene como objetivo ayudar al usuario a comprender el impacto del deslizamiento (*slippage*) y las comisiones al realizar operaciones en mercados con distintos niveles de profundidad y liquidez.

Cálculo con VWAP

El algoritmo utilizado en el simulador se basa en el cálculo del **VWAP** (*Volume Weighted Average Price*), que representa el precio promedio ponderado por volumen al cual se ejecutaría una orden de mercado sobre el libro de órdenes.

- En una operación de tipo `buy`, el sistema recorre progresivamente los niveles de *ask* (ofertas de venta), acumulando volúmenes hasta alcanzar la cantidad deseada.
- En una operación de tipo `sell`, se recorren los niveles de *bid* (ofertas de compra) con la misma lógica.

Este procedimiento garantiza una simulación precisa y cercana a la realidad operativa de un usuario que utiliza órdenes de mercado en los exchanges disponibles.

Parámetros considerados en cada simulación

Cada simulación se realiza considerando de forma uniforme los siguientes elementos para todos los exchanges:

- **VWAP**: calculado dinámicamente a partir del volumen y precio de cada nivel del libro de órdenes.
- **Comisión de tipo *taker***: definida por cada exchange y almacenada en el archivo de configuración general del sistema.
- **Total final de la operación**: monto neto que se pagaría o recibiría, considerando el precio promedio y la comisión.

Comparación directa entre exchanges

Luego de ejecutar la simulación para cada exchange de forma independiente, el sistema muestra al usuario una tabla con los resultados. Esto permite visualizar cuál sería el rendimiento de ejecutar el 100 % de la orden en cada uno.

Tabla 3: Comparación entre exchanges – simulación 100 % de la orden (ejemplo ilustrativo)

Exchange	Precio Prom.	Fee	Total Final
Binance	2738.74	273.87	273600.08
KuCoin	2738.46	273.85	273572.06
Kraken	2739.12	712.33	274201.45
Coinbase	2744.17	1646.50	276064.39

Nota: los valores anteriores corresponden a un ejemplo ejecutado en una fecha específica. La volatilidad de los mercados puede hacer que los resultados varíen significativamente en el tiempo.

Ventajas y limitaciones de esta simulación

Esta simulación proporciona al usuario una referencia confiable para comparar los exchanges bajo las mismas condiciones de mercado. Sin embargo, al considerar únicamente ejecuciones del 100 % en un solo exchange, no necesariamente representa la estrategia más eficiente.

En la práctica, una combinación óptima de asignaciones parciales en varios exchanges puede minimizar el costo total o maximizar el retorno. Por este motivo, el simulador se complementa con un módulo de optimización, descrito en la siguiente sección, el cual analiza múltiples distribuciones posibles para encontrar la mejor solución global.

Optimización de Órdenes

Además del análisis individual por exchange, el sistema cuenta con un módulo de optimización diseñado para encontrar la distribución óptima de una orden entre múltiples exchanges, con el fin de maximizar el retorno (en una venta) o minimizar el costo (en una compra).

Propósito y enfoque del optimizador

Dado que los diferentes exchanges presentan variaciones en sus libros de órdenes, niveles de liquidez y comisiones, ejecutar una orden completa en un solo exchange puede no ser la mejor estrategia. El optimizador busca distribuir la cantidad total a operar entre dos o más exchanges, evaluando el impacto conjunto de:

- Precio promedio ponderado por volumen (VWAP).
- Estructura de comisiones (*taker fees*).
- Profundidad y forma del libro de órdenes.

A diferencia de la simulación individual, el optimizador considera múltiples combinaciones posibles de asignación de volumen, bajo un esquema de búsqueda continua dentro del intervalo [0, 1] para cada exchange, sujeto a que la suma total sea igual al 100 % de la orden.

Evaluación de escenarios

Para cada combinación evaluada, el sistema simula parcialmente la ejecución de la orden en cada exchange, calcula los costos o ingresos netos, y selecciona la distribución que arroje el mejor resultado global.

Este enfoque permite captar pequeñas ventajas en precios o comisiones entre exchanges, lo cual resulta especialmente útil en mercados de alta volatilidad o bajo volumen.

Ejemplo ilustrativo

A continuación se presenta un ejemplo de optimización para una orden de compra de 100 ETH, considerando cuatro exchanges en tiempo real:

Tabla 4: Resultado de la optimización – distribución entre exchanges (ejemplo)

Exchange	**Precio Prom.**	**Fee**	**Total Final**	**% Óptimo**	**Cantidad**
Binance	2740.87	137.04	137180.47	50.00 %	50.000004 ETH
KuCoin	2740.69	137.03	137171.62	50.00 %	49.999996 ETH
Kraken	-	-	-	0.00 %	0.000000 ETH
Coinbase	-	-	-	0.00 %	0.000000 ETH
Total	–	–	**274352.09 USDT**	100 %	100.0 ETH

Nota: este ejemplo representa un caso real ejecutado en el sistema. Las asignaciones reflejan que Binance y KuCoin ofrecían en conjunto el mejor resultado, mientras que Kraken y Coinbase fueron descartados por su menor competitividad en ese momento.

Utilidad práctica

Esta optimización automatizada permite a traders o sistemas algorítmicos tomar decisiones más eficientes, eliminando la necesidad de evaluar manualmente múltiples escenarios. Es particularmente útil para:

- Operaciones de gran volumen que puedan causar deslizamiento significativo.
- Escenarios donde pequeños márgenes hacen la diferencia (arbitraje, market making).
- Análisis comparativo para decidir rutas de operación entre plataformas.

El resultado del optimizador puede visualizarse gráficamente para facilitar su interpretación, como se explica en la siguiente sección.

Universidad de los Andes

Capítulo 4

Resultados y discusiones

En esta sección se presentan los resultados obtenidos al ejecutar el sistema de optimización y simulación en un escenario real utilizando libros de órdenes en tiempo real. El objetivo es demostrar cómo varían los resultados al ejecutar una orden completa en un solo exchange frente a distribuirla estratégicamente entre varios. Se incluye un análisis comparativo de las alternativas evaluadas.

Ejemplo 1: Compra de 100 ETH

Se simuló la ejecución de una orden de **compra de 100 ETH** en los exchanges Binance, KuCoin, Kraken y Coinbase, evaluando tanto la ejecución completa en cada uno como la distribución óptima entre ellos.

Simulación 100 % por exchange

La primera fase del experimento consiste en simular la compra del total de los 100 ETH en cada exchange, utilizando el libro de órdenes disponible al momento de la prueba. La siguiente tabla muestra el resultado de ejecutar esta orden completa por separado en cada plataforma:

Tabla 5: Comparación entre exchanges – ejecución completa de la orden

Exchange	**Precio Prom.**	**Fee (USDT)**	**Total Final (USDT)**
Binance	2740.50	274.05	274324.23
KuCoin	2740.76	274.08	274349.86
Kraken	2740.83	712.62	274795.51
Coinbase	2743.57	1646.14	276003.02

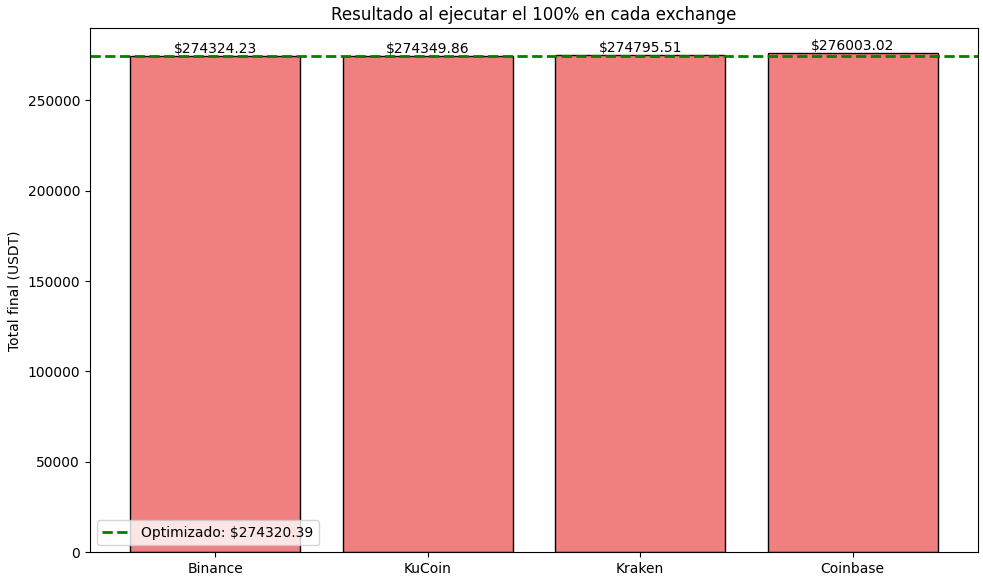

Figura 2: Comparación visual del total a pagar al comprar 100 ETH en un solo exchange

Optimización multi-exchange

Luego se ejecutó el algoritmo de optimización con el objetivo de minimizar el total pagado por la compra, permitiendo dividir la orden entre múltiples exchanges. El resultado obtenido se presenta a continuación:

Tabla 6: Distribución óptima para la compra de 100 ETH

Exchange	**Precio Prom.**	**Fee**	**Total Final**	**% Óptimo**	**ETH Asignado**
Binance	2740.44	137.02	137159.02	50.0 %	50.0 ETH
KuCoin	2740.49	137.03	137161.32	50.0 %	50.0 ETH
Kraken	2740.57	0.0001	0.05	0.0 %	0.000017 ETH
Coinbase	–	0.0	0.0	0.0 %	0.0 ETH
TOTAL	**274320.39 USDT**				

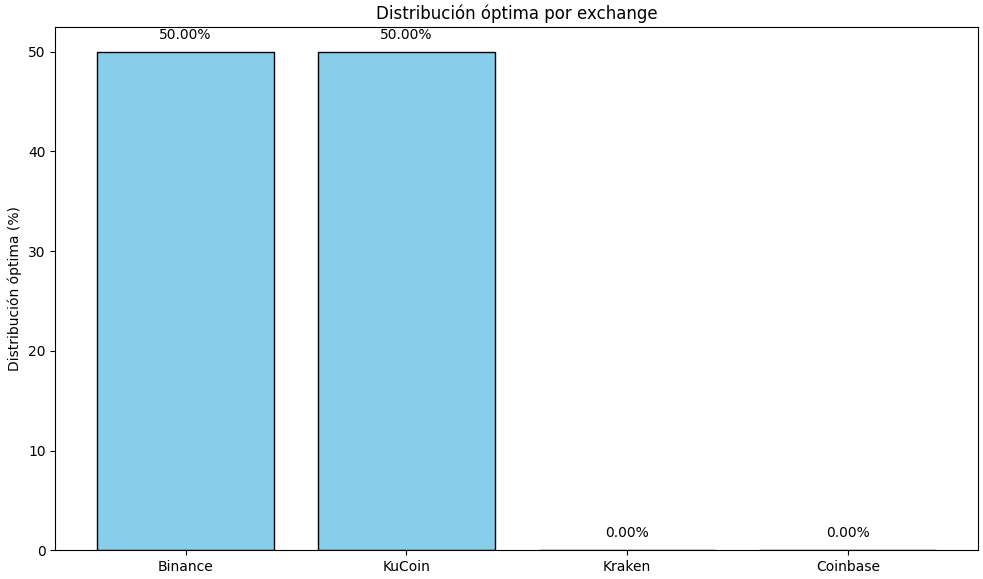

Figura 3: Distribución óptima de la compra de 100 ETH entre los exchanges

Análisis del resultado

Este caso muestra claramente las ventajas de la estrategia de optimización. A pesar de que la diferencia entre los exchanges no es drásticamente amplia, la distribución óptima logró reducir el costo total de la operación.

- La mejor opción individual fue Binance, con un costo de 274324.23 USDT por los 100 ETH.
- Al dividir la orden en partes iguales entre Binance y KuCoin, el sistema logró un costo optimizado de 274320.39 USDT, es decir, una mejora de aproximadamente 3.84 USDT.
- Exchanges como Kraken y Coinbase fueron descartados automáticamente por el optimizador debido a su alta comisión o precio promedio menos favorable.

Aunque el ahorro puede parecer marginal, este comportamiento se amplifica en operaciones más grandes o en sistemas que realizan transacciones de alta frecuencia, donde cada punto decimal representa un valor significativo acumulado en el tiempo.

Además, este resultado valida la precisión de los algoritmos desarrollados, ya que el uso de VWAP, junto con una simulación fiel al libro de órdenes, permite tomar decisiones informadas incluso bajo condiciones de mercado en tiempo real.

Ejemplo 2: Venta de 150 ETH

En este segundo experimento, se simuló una operación de **venta de 150 ETH**, nuevamente comparando los resultados de realizar la operación en su totalidad en un solo exchange frente a utilizar el algoritmo de distribución óptima entre múltiples plataformas.

Simulación 100 % por exchange

A continuación se muestra la tabla con los resultados obtenidos al vender los 150 ETH en cada uno de los exchanges de forma individual, utilizando el libro de órdenes en tiempo real:

Tabla 7: Comparación entre exchanges – ejecución completa de la venta

Exchange	Precio Prom.	Fee (USDT)	Total Final (USDT)
Binance	2739.61	410.94	410531.17
KuCoin	2738.80	410.82	410408.92
Kraken	2739.78	1068.52	409899.04
Coinbase	2736.46	2462.81	408005.61

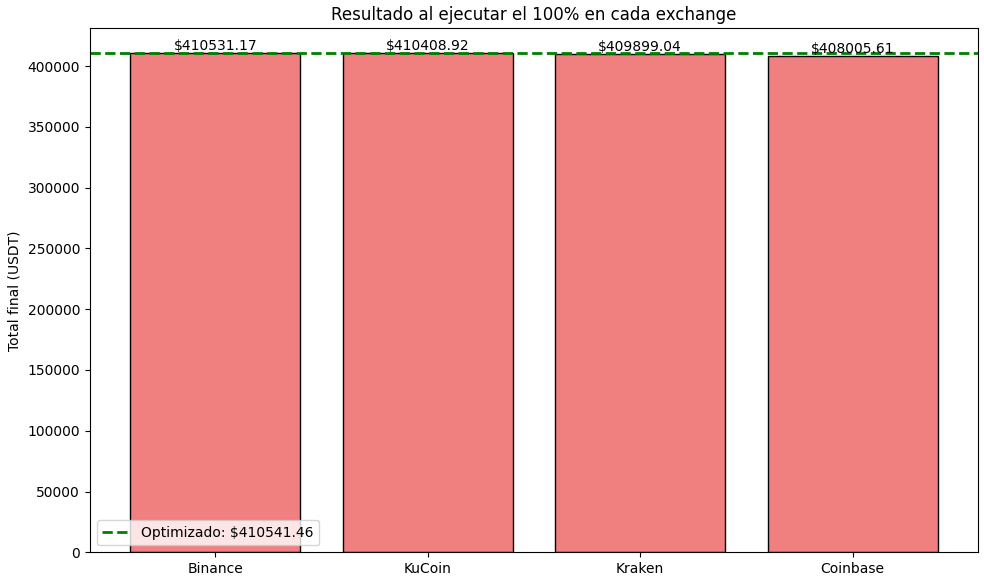

Figura 4: Comparación visual del total recibido al vender 150 ETH en un solo exchange

Optimización multi-exchange

El algoritmo de optimización calculó la distribución ideal de la venta entre exchanges con el objetivo de maximizar el valor recibido en USDT. Los resultados se presentan en la siguiente tabla:

Tabla 8: Distribución óptima para la venta de 150 ETH

Exchange	Precio Prom.	Fee	Total Final	% Óptimo	ETH Asignado
Binance	2739.74	283.61	283326.69	69.01 %	103.52 ETH
KuCoin	2739.55	127.34	127214.74	30.99 %	46.48 ETH
Kraken	2740.46	0.0001	0.03	0.0 %	0.000013 ETH
Coinbase	–	0.0	0.0	0.0 %	0.0 ETH
TOTAL	**410541.46 USDT**				

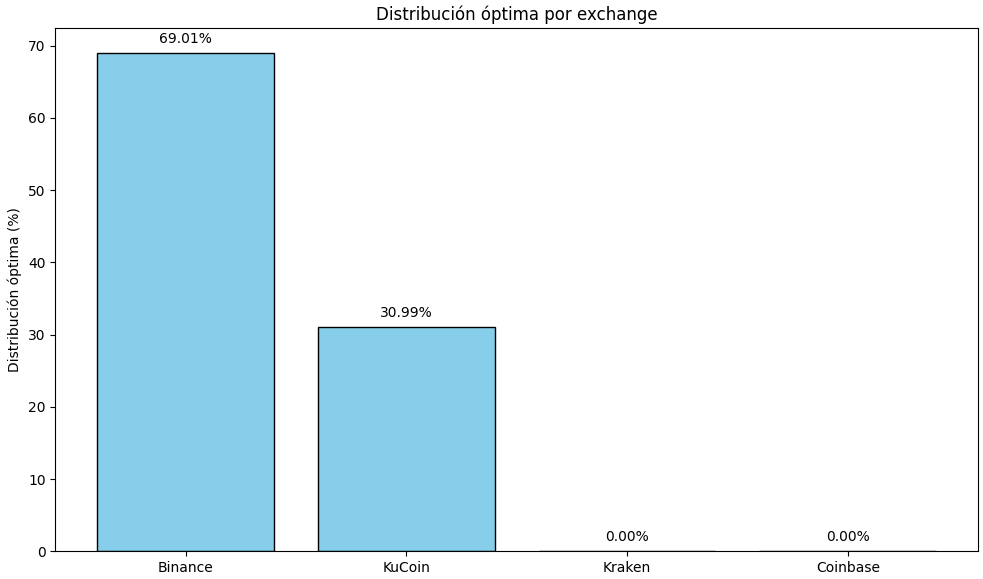

Figura 5: Distribución óptima de la venta de 150 ETH entre los exchanges

Análisis del resultado

Los resultados reflejan el impacto que puede tener la fragmentación inteligente de una orden:

- El mejor exchange individual fue Binance, con un ingreso neto de 410531.17 USDT.

- El algoritmo distribuyó la orden de forma estratégica, asignando el 69 % del volumen a Binance y el 31 % a KuCoin, obteniendo así un ingreso optimizado total de **410541.46 USDT**, mejorando el resultado en más de **10 USDT**.

- Tanto Kraken como Coinbase fueron descartados por el optimizador, debido a sus comisiones más altas y menor ventaja relativa.

A pesar de que la mejora absoluta en este caso es menor al 0.003 %, sigue siendo significativa en contextos de trading automático, arbitraje o plataformas institucionales, donde grandes volúmenes y operaciones recurrentes amplifican el beneficio acumulado. Además, estos resultados validan la importancia de la ejecución inteligente basada en libros de órdenes y algoritmos de optimización.
Los resultados obtenidos en los casos de estudio permiten evidenciar el funcionamiento y utilidad del optimizador desarrollado. A través de la simulación de órdenes completas y la distribución estratégica de volúmenes entre exchanges, se demuestra que el sistema puede identificar combinaciones de plataformas que ofrecen mejores resultados que cualquier ejecución única. Este tipo de optimización cobra especial relevancia cuando se integra con agentes automáticos de trading, en donde las operaciones se ejecutan de forma continua y en intervalos muy cortos. En contextos de alta frecuencia, incluso pequeñas mejoras en el rendimiento de cada operación representan ahorros significativos a gran escala, lo que convierte a este tipo de herramientas en componentes valiosos para cualquier estrategia cuantitativa. No obstante, es importante señalar que dado que el análisis se realiza en tiempo real sobre libros de órdenes dinámicos, los resultados entregados por el simulador y el optimizador son aproximaciones. Aunque se basan en información precisa del momento de ejecución, no pueden garantizar resultados exactos debido a la naturaleza cambiante de los mercados. Aun así, ofrecen una base sólida y confiable para la toma de decisiones informadas en entornos altamente volátiles..

Universidad de los Andes

Capítulo 5

Conclusiones y trabajo futuro

Este capítulo analiza los hallazgos del proyecto desde una perspectiva crítica, explorando sus implicaciones técnicas, estratégicas y prácticas para Peccala y el ecosistema cripto en general. También se abordan las limitaciones del sistema propuesto, así como posibles mejoras para su escalabilidad y sostenibilidad en el tiempo.

Análisis de Resultados

El desarrollo del sistema permitió simular múltiples escenarios de envío de fondos y ejecución de órdenes en distintos entornos blockchain y exchanges. Los casos planteados demuestran que, al contar con una herramienta de análisis en tiempo real, es posible tomar decisiones más eficientes que las que se podrían lograr mediante métodos manuales o intuitivos. En el caso del módulo de trading, se confirmó que el *slippage* en órdenes grandes puede reducirse significativamente si se diversifica la operación entre varios exchanges. La comparación entre la ejecución 100 % en un solo exchange y la optimización multiexchange basada en el cálculo de VWAP demostró que los resultados financieros pueden mejorar, aunque sea por márgenes pequeños, lo que resulta estratégico en escenarios de alta frecuencia. Por ejemplo, en una orden de compra de 100 ETH, el optimizador fue capaz de distribuir el volumen entre Binance y KuCoin, maximizando el número de tokens adquiridos respecto a cualquier ejecución individual. En el caso de una orden de venta de 150 ETH, el sistema asignó el volumen de forma asimétrica, priorizando los exchanges con mejor liquidez efectiva y menores comisiones, lo que resultó en un ingreso total más alto. Este tipo de distribución no sería viable mediante decisiones humanas en tiempo real, dado el dinamismo de los libros de órdenes y los cambios constantes en precios y profundidades. El sistema automatizado ofrece una ventaja competitiva significativa en este contexto.

Implicaciones Técnicas

Desde una perspectiva técnica, el sistema desarrollado demuestra que es posible construir soluciones de análisis en tiempo real utilizando exclusivamente las APIs públicas de los exchanges. La integración exitosa con Binance, KuCoin, Kraken y Coinbase permitió validar la capacidad del modelo para acceder a datos de libros de órdenes en tiempo real, calcular métricas relevantes como el VWAP y simular operaciones con precisión. Sin embargo, este proceso también reveló varios desafíos importantes:

- **Variabilidad de datos:** Las respuestas de las APIs cambian en fracciones de segundo, por lo que cualquier análisis representa un estado puntual del mercado. Esto exige una alta frecuencia de consulta y una gestión cuidadosa de la latencia.
- **Limitaciones de las APIs:** Algunos exchanges imponen límites estrictos en la tasa de consultas (*rate limit*), y otros, como Coinbase, no ofrecen libros de órdenes con suficiente profundidad para simular grandes volúmenes de manera realista.
- **Heterogeneidad en los formatos:** Cada proveedor utiliza convenciones distintas para representar símbolos, niveles de profundidad y precios. Fue necesario implementar múltiples capas de estandarización para convertir los datos a un formato común antes de ejecutar los cálculos.
- **Comisiones específicas por exchange:** Las tarifas de taker varían entre plataformas, y algunas dependen del volumen de operaciones del usuario. El sistema incorporó estas comisiones de forma parametrizable para reflejar escenarios más realistas.

A pesar de estas complejidades, el sistema demostró ser robusto, modular y confiable en todas las pruebas realizadas, generando simulaciones precisas que pueden servir como base para decisiones automatizadas.

Limitaciones del Proyecto

Si bien el sistema cumple su objetivo de brindar un análisis detallado de órdenes de compra y venta en tiempo real a través de múltiples exchanges, presenta ciertas limitaciones que deben considerarse:

- **No ejecución real de operaciones:** El sistema está diseñado como una herramienta de simulación y optimización, por lo que no interactúa con billeteras, firmas digitales ni ejecuta órdenes reales en exchanges. Su objetivo es informativo, no transaccional.
- **Dependencia del estado instantáneo del mercado:** Las simulaciones se realizan con base en un snapshot puntual del libro de órdenes. Dado que los mercados son altamente volátiles, los resultados deben interpretarse como aproximaciones válidas en ese instante, pero no como predicciones a futuro.
- **Cobertura limitada de exchanges:** Aunque el sistema ya incluye cuatro exchanges importantes (Binance, KuCoin, Kraken y Coinbase), no todos los exchanges ofrecen APIs abiertas, profundidad completa en el libro de órdenes o formatos estandarizados. La escalabilidad del sistema a más plataformas requerirá desarrollos adicionales.

- **Ausencia de técnicas predictivas:** El sistema no incorpora modelos de aprendizaje automático o predicción de precios. Todos los cálculos se realizan sobre datos actuales, sin considerar movimientos esperados del mercado ni señales técnicas.
- **Interfaz de usuario mínima:** La herramienta fue desarrollada en entorno de consola para facilitar pruebas y validación técnica. Aún no cuenta con una interfaz gráfica ni se ha integrado con un sistema de monitoreo automatizado.

Estas limitaciones no afectan la validez de las simulaciones realizadas, pero sí acotan el alcance práctico de la herramienta en un entorno productivo. No obstante, todas representan oportunidades claras para trabajos futuros.

Impacto Estratégico para Peccala

El sistema desarrollado presenta un alto potencial de impacto en los procesos internos de Peccala, especialmente en su estrategia de trading automatizado y gestión activa de portafolios en múltiples exchanges y blockchains. La capacidad de simular y optimizar órdenes en tiempo real permite una toma de decisiones más precisa, con menor margen de error operativo y mayor control sobre los costos asociados.

- **Ahorro acumulativo en operaciones de alta frecuencia:** Aunque las diferencias de optimización por orden pueden parecer marginales, en un entorno donde se realizan cientos o miles de operaciones al día, estos márgenes representan ahorros significativos en el tiempo.
- **Mejora en el control del slippage:** La herramienta permite evaluar anticipadamente el impacto del slippage en órdenes grandes, facilitando la diversificación entre exchanges y la mitigación de pérdidas asociadas a baja liquidez.
- **Soporte a la toma de decisiones automatizada:** El diseño modular del sistema lo hace ideal para integrarse en pipelines de trading algorítmico o herramientas de apoyo a traders, incrementando la capacidad de reacción ante cambios abruptos en el mercado.
- **Base técnica para desarrollos futuros:** Esta herramienta puede convertirse en el núcleo de sistemas más avanzados que incluyan inteligencia artificial, predicción de mercado, conexión con wallets seguras y ejecución automatizada.

En resumen, la herramienta ofrece ventajas estratégicas tangibles para Peccala, tanto en eficiencia operativa como en la capacidad de escalar su infraestructura técnica en el futuro cercano.

Potencial de Aplicación Generalizada

Aunque este proyecto fue desarrollado con un enfoque específico hacia las operaciones de Peccala, su arquitectura modular y su enfoque técnico permiten una adopción mucho más amplia. Cualquier entidad que realice trading de criptoactivos o transferencias frecuentes entre redes y exchanges puede beneficiarse directamente de este tipo de herramientas.

- **Startups y fondos de inversión:** Empresas emergentes en el sector DeFi pueden utilizar esta solución para reducir sus costos operativos y mejorar la eficiencia en el manejo de portafolios multicadena.
- **Traders profesionales y creadores de mercado:** Aquellos que operan con alta frecuencia pueden integrar este sistema como parte de sus herramientas de análisis para automatizar decisiones informadas, ahorrando en slippage y comisiones.
- **Analistas financieros y educadores:** El simulador y el optimizador pueden emplearse como material didáctico o herramienta de análisis, facilitando la enseñanza y la exploración de fenómenos como la liquidez de mercado, la profundidad de libro o el comportamiento de las comisiones.
- **Integraciones con wallets y dApps:** A futuro, este sistema podría incorporarse en interfaces gráficas o billeteras digitales que permitan a los usuarios ejecutar operaciones informadas con solo unos clics, mejorando la transparencia y el control para usuarios minoristas.
- **Gobiernos o reguladores financieros:** En entornos que buscan monitorear el mercado cripto, este tipo de herramientas podría ser adaptado como sistema de vigilancia y análisis de comportamiento en tiempo real.

Así, el sistema desarrollado no solo representa una solución técnica puntual, sino una plataforma con capacidad de adaptarse y escalar hacia diferentes tipos de usuarios, industrias y casos de uso dentro del ecosistema blockchain global.

Universidad de los Andes

Repositorio del proyecto

Para fomentar la transparencia, replicabilidad y el desarrollo colaborativo, el código fuente completo del sistema desarrollado se encuentra disponible públicamente en el siguiente repositorio:
`https://github.com/juaneslava/optimizador_PDG_JESLAVA_ASEGURAT202501-`

Este repositorio contiene todos los módulos necesarios para la simulación de transferencias y la optimización de órdenes, ejemplos reproducibles, scripts de generación de gráficos, instrucciones de instalación y documentación técnica complementaria. De esta forma, se busca que investigadores, estudiantes o profesionales interesados puedan replicar, auditar o extender este trabajo fácilmente.

Universidad de los Andes

Bibliografía

[1] Xiang Fu, Huaimin Wang y Peichang Shi. "A survey of Blockchain consensus algorithms: mechanism, design and applications". En: *Science China Information Sciences* 64.121101 (2021). DOI: 10.1007/s11432-019-2790-1. URL: https://link.springer.com/article/10.1007/s11432-019-2790-1.

[2] Joshua S. Gans y Neil Gandal. "Consensus Mechanisms for the Blockchain". En: *The Palgrave Handbook of Technological Finance* (2021), págs. 269-286. DOI: 10.1007/978-3-030-65117-6_11. URL: https://ideas.repec.org/h/spr/sprchp/978-3-030-65117-6_11.html.

[3] Fireblocks. *Fireblocks: Digital Asset Custody and Treasury Management*. 2023. URL: https://www.fireblocks.com/digital-asset-custody/.

[4] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2017. URL: https://books.google.com/books/about/Mastering_Bitcoin.html?id=tponDwAAQBAJ.

[5] Vitalik Buterin. *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform*. 2013. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

[6] LI.FI. *LI.FI API Documentation*. 2023. URL: https://docs.li.fi/li.fi-api/li.fi-api.

[7] Mo Dong et al. "Celer Network: Bring Internet Scale to Every Blockchain". En: *arXiv preprint arXiv:1810.00037* (2018). URL: https://arxiv.org/abs/1810.00037.

[8] Binance. *Binance API Documentation*. 2023. URL: https://developers.binance.com/docs/binance-spot-api-docs/rest-api.

[9] KuCoin. *KuCoin API Documentation*. 2023. URL: https://www.kucoin.com/docs-new/introduction.

[10] Kraken. *Kraken API Documentation*. 2023. URL: https://docs.kraken.com/.

[11] Irene Aldridge. "Slippage in AMM Markets". En: *SSRN Electronic Journal* (2022). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4133897.

[12] Coinbase. *Coinbase API Reference*. 2023. URL: https://docs.cloud.coinbase.com/exchange/docs.

[13] CoinMarketCap Alexandria. *Understanding VWAP and Slippage in Crypto Markets*. 2023. URL: https://coinmarketcap.com/alexandria/article/what-is-vwap-in-crypto.

[14] Kenneth Reitz. *Requests: HTTP for Humans*. 2023. URL: https://docs.python-requests.org/en/latest/.

[15] The Matplotlib Development Team. *Matplotlib Documentation*. 2023. URL: https://matplotlib.org/stable/contents.html.

[16] SciPy Community. *SciPy Optimize Documentation*. 2023. URL: https://docs.scipy.org/doc/scipy/reference/optimize.html.