PROYECTO 1.

Monitor de criptomonedas digitales.

Semestre Abril-Agosto-2021

Documento Versión 1

Fase 1.

El objetivo desde el punto de vista del docente es evaluar los conocimientos adquiridos por el estudiante en la aplicación de los principios de la programación orientada a objeto para la implementación de algoritmos, así como también el análisis y diseño usando para la solución de problemas herramientas de modelado UML.

Para estar a la vanguardia en el desarrollo de aplicaciones, se ha considerado al grupo de la materia de Algoritmos III el desarrollo de una aplicación para monitorear en tiempo real información básica sobre criptomonedas así como también agregar un conjunto de requerimientos que nos permitan poder tomar decisiones al momento de comprar o vender una moneda digital del portafolio que pueda tener un usuario de la aplicación.

Como es bien conocido el mundo de las monedas digitales o criptomonedas son proyectos que están respaldados por una moneda que intenta monetizar un proyecto tecnológico, comenzando por la primera: BITCOIN que junto a su blockchain han revolucionado el mercado de las finanzas, inversiones, servicios y un sinfín de usos más, tomando como principales características: la descentralización, rapidez e la inmutabilidad de las transacciones, seguridad, transparencia y algo muy importante a nivel humano: cada quien es su propio banco ya que no dependes de instituciones financieras.

Bitcoin y al igual que cualquier criptomoneda que pasa de ser un proyecto a tener una ICO (Initial coin offer, el principio de la búsqueda de financiación de la idea con la participación de cualquier persona en la compra de sus monedas[i]) al tener su precio referido en dinero FIAT [ii](del latín *fiat*, 'hágase) que proviene del estado, ejemplos de dinero fiat: dólar, euro, entre otras monedas de reserva[iii], comienza todo el movimiento especulativo en mercados financieros que en este caso se realiza por los Exchange[iv] que son las plataformas que permiten el comercio entre los usuarios en las distintas criptomonedas.

Bitcoin

Bitcoin la primera criptomoneda fue creada por Satoshi Nakamoto, que para la fecha nadie sabe quién es, si es una persona, un grupo de ellas o un nombre inventado, lo cierto del caso es su creador tiene alrededor de un millón de bitcoins (para la fecha supera los 10.000 millones) actualmente que fueron minados por él mismo en los primeros siete meses de existencia de BTC[v], como se escribió anteriormente cada criptomoneda está respaldada por un proyecto tecnológico lo cual está documentado en lo que se conoce como el "White Paper"[vi], en el sitio oficial de Bitcoin: bitcoin.org se puede leer el White paper[vii] que ha revolucionado el mundo financiero a nivel tecnológico.

Acrónimo de las criptomonedas

Cada Criptomoneda tiene un acrónimo que la identifica (en el mundo financiero se le conoce como ticket), el de BITCOIN es BTC, el de ETHEREUM es ETH, RIPPLE es XRP etc.

Satoshi

Al igual que un Bit es la mínima unidad de medida de información en el computador (la cual es binaria: ceros y unos), en BTC la mínima unidad de medida se conoce como SATOSHI. Cada BTC es divisible por 100.000.000 de "céntimos" llamados satoshi, y permite reflejar saldos de hasta ocho decimales, por lo tanto 1 BTC = 1,00000000 y un Satoshi es 0,00000001.

Monedas estables

Son monedas que están "respaldadas en el dólar", una unidad de estas monedas son equivalentes de manera muy aproximada a 1 $ (con un margen muy pero muy pequeño), ejemplos de ellas son: USDT (Tether), USDC, DAI.

Market Cap (capitalización del mercado)[viii]

Es la capitalización bursátil de una criptomoneda, permite clasificar la dimensión de una criptomoneda y se calcula multiplicando el precio por la cantidad de monedas circulantes. Para la creación de este documento la capitalización del mercado para bitcoin es de 695.851.481.125$ con un precio por BT de 37.198,70 y una cantidad circulante de 18.731.218 BTC (es necesario acotar que la cantidad máxima que tendrá BTC es de 21.000.000 de unidades).[ix] Se estima que el último Bitcoin se minará en el año 2140. Más información interesante en el siguiente enlace: https://www.ig.com/es/bitcoin/bitcoin-halving

Para conocer más sobre los términos del mundo cripto pueden visitar el siguiente enlace: https://blockchainespana.com/glosario/, https://academy.bit2me.com/diccionario-crypto/, https://www.finder.com/mx/glosario-de-criptomonedas.

Y…..Qué se quiere desarrollar?

El objetivo de la aplicación que se desea desarrollar en esta primera fase, es crear una herramienta que permita obtener datos de las principales 10 criptomonedas del mercado (las de mayor capitalización), así como también poder agregar alertas de precios, para que se activen cuando Bitcoin alcance un precio dado por el usuario, todo esto en tiempo real.

Funcionalidades principales.

Registro de usuario.

Permite el registro de usuario en la aplicación, se debe solicitar al usuario el correo (debe ser un correo sintácticamente valido, usar expresiones regulares) y un password que debe ser mayor a ocho caracteres debe incluir caracteres, números, una letra mayúscula y un carácter especial, estos datos se deben registrar en formato JSON en un archivo plano, la clave debe guardarse de manera cifrada. Si el usuario coloca un correo ya registrado, la aplicación debe indicar que ya esta registrado y por supuesto hacer las validaciones al dejar los datos en blanco.

Autenticación de usuario.

Permite al usuario ingresar al área privada de la aplicación mediante el correo y el password. Si el usuario no está autenticado solo se muestra la información de Bitcoin y no podrá hacer más nada, solo registrarse o salir de la aplicación.

Modificación de datos de acceso.

Permite modificar la contraseña, para ello debe colocarse la contraseña vieja y colocar la nueva con su respectivo campo de conformación y las mismas validaciones indicadas en el registro. Para modificar la contraseña debe estar autenticado.

Listado de las 10 criptomonedas con mayor market cap en el momento.

Muestra un listado con las 10 monedas de mayor capitalización e información relacionada con cada una de ellas, esta información es:

Moneda, ticket, precio actual, market cap, volumen de las últimas 24 horas, cantidad de monedas circulantes, margen de pérdida o ganancia en: la última hora, 4 horas (solo si el api seleccionada lo permite), un día y 7 días.

Alertas.

Permite crear alertas que deben activarse cuando el precio de Bitcoin alcance el precio indicado en la alerta. El precio de una criptomoneda al igual que cualquier índice financiero, activo, divisa entre otros, varia su precio por la ley de oferta y demanda. Con esta funcionalidad el usuario indica un precio y cuando BTC alcance ese precio se debe activar un sonido y mostrar la alerta que el usuario creo.

Ejemplo: supongamos que BTC está en el precio de 37.500$/BTC, el usuario decide crear una alerta al precio de 37.000$/BTC, la aplicación debe estar corriendo y monitoreando en tiempo real el precio de la moneda cuando el precio supere hacia abajo los 37.000$/BTC la alerta se activa y se muestra en la aplicación con una interfaz anunciando que la alerta se activó y emitir un sonido seleccionado por el usuario previamente, ***la alerta continuará mostrándose hasta que el usuario presione un botón para detener la alerta.***

Se establecen 6 sonidos por defecto y únicos para que el usuario pueda seleccionar cualquier de ellos para la alerta que esta creando.

Una alerta se puede modificar y/o eliminar, pueden existir tantas alertas como el usuario desee. Si el usuario quiere editar una alerta, la debe seleccionar de la lista y puede cambiar el precio y el sonido.

Al procesar una modificación o eliminación de alerta, se debe mostrar el mensaje respectivo más los datos modificados o eliminados.

Cada vez que se crea un alerta se debe verificar que el usuario este autenticado (logeado) sino lo está debe emitirse un mensaje indicando que debe autenticarse, esto se puede eviar no mostrando la opción de creación de alerta al entrar a la aplicación.

Si el usuario no está autenticado la alerta no emite información al usuario de llegar a dispararse.

La aplicación debe contar con una opción para salir del área privada la cual al usarla debe verificar con el usuario si está seguro o no, de ser positivo, solo se lleva a mostrar el precio de bitcoin y las opciones de: Autenticación, registro y salir.

Restricciones:

Toda la información debe guardarse en archivos de texto plano en formato JSON, cada vez que el usuario: registra, define una alerta, se autentica (guarda fecha, hora e IP del computador donde se autentico) esta debe actualizarse en archivos de texto.

Cada vez que se ejecute el programa se carga toda la información que está en el o los archivos de texto en las respectivas estructuras de datos.

Para mostrar información de las criptomonedas, se debe usar una API (librería/servicio) que permite obtener dicha información, ejemplo: CoinMarketCap API: https://coinmarketcap.com/api/, para hacer uso de esta API se debe trabajar con la librería: APACHE HTTP Components versión: 4.5.13.

Grupos de proyecto:

- El grupo de proyecto debe ser realizado por 3 personas, los mismos deben estar presentes para la defensa del proyecto y se corrige individualmente.

Características técnicas.

- El programa debe ser implementado en JAVA usando Programación Orientada a Objeto, aplicando los principios vistos en clase: DRY YAGNI, KISS Y SOLID, estos principios serán evaluados.
- Se deben seguir los estándares vistos en clase para la codificación.

Fecha Entrega (del 05/07/2021 al 09/07/2021) 20%

- Documentos a entregar:
  - Diagrama de casos de uso.
  - Diagrama de clases.
  - Diagrama de componentes.
  - Descripción de las API externas necesarias para la ejecución del proyecto.
  - Guía de instalación y uso del software (Si es necesario).
  - El software debe estar documentado de manera completa usando JAVADOC.

---

[i] ICO: https://academy.bit2me.com/ico-criptomonedas/

[ii] FIAT: https://www.moneyman.es/blog/que-es-el-dinero-fiat/

[iii] Monedas de reserva: https://es.wikipedia.org/wiki/Moneda_de_reserva

[iv] Exchange: https://academy.bit2me.com/que-es-exchange-criptomonedas/

[v] Cuantos BTC tiene Satoshi? https://decrypt.co/es/53066/cuantos-bitcoin-tiene-satoshi-nakamoto

[vi] White paper: https://rockcontent.com/es/blog/white-paper/

[vii] White paper de bitcoin: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

[viii] Market Cap: https://coinmarketcap.com/es/faq/

[ix] Cuantos Btc hay? https://www.buybitcoinworldwide.com/es/cuantos-bitcoins-hay/

CIFRADO AES-128:
https://programmerclick.com/article/2306644480/#:~:text=AES%3A%20Advanced%20Encryption%20Standard%20(Advanced,debe%20guardarse%20y%20no%20filtrarse.&text=El%20front%2Dend%20aplica%20una,para%20descifrar%20la%20clave%20AES.