Descripción General

El contrato implementa una subasta en la blockchain de Ethereum, donde los usuarios pueden ofertar por un bien o servicio. El contrato gestiona las ofertas, depósitos, extensiones automáticas del tiempo de subasta, retiros de fondos y comisiones, asegurando transparencia y seguridad para todas las partes involucradas.

Detalle de Funcionamiento

1. Inicialización

El propietario (owner) despliega el contrato y define la duración de la subasta en días.

Se establece el tiempo de finalización (auctionEndTime) y se inicializan las variables de control.

2. Ofertas (bid)

Cualquier usuario, excepto el propietario, puede ofertar enviando ETH.

La nueva oferta debe ser al menos un 5% mayor que la oferta más alta actual.

Si la oferta se realiza cerca del final (últimos 10 minutos), la subasta se extiende automáticamente hasta un máximo de 7 días.

Se actualizan los registros de depósitos y el historial de ofertas.

El mejor postor y la oferta más alta se actualizan en cada nueva oferta válida.

3. Retiros Parciales (partialWithdraw)

Mientras la subasta está activa, los ofertantes pueden retirar cualquier exceso de depósito que no esté incluido en su última oferta.

4. Retiros de Depósito tras la Subasta (withdrawDeposit)

Cuando la subasta termina, los ofertantes que no ganaron pueden retirar su depósito, menos una comisión del 2% que se transfiere al propietario.

El ganador no puede retirar su depósito, ya que este corresponde al pago de la subasta.

Escalable: no depende de la cantidad de participantes.

- Utilizo esta funcion porque es segura: el usuario inicia la transacción, evitando problemas de gas y ataques de denegación de servicio. el modelo push (que no es recomendable para subastas publicas). Tiene como ventaja que los usuarios no precisan realizar nada para recibir su reembolso. **Riesgo de denegación de servicio:** Si un usuario es un contrato malicioso o rechaza ETH, puede hacer que toda la función falle. **Límites de gas:** Si hay muchos participantes, la transacción puede quedarse sin gas y revertir.

5. Finalización y Cancelación

El propietario puede finalizar la subasta manualmente antes del tiempo límite. El propietario puede cancelar la subasta solo si no se han realizado ofertas.

6. Retiro de Fondos por el Propietario (withdrawFunds)

Tras finalizar la subasta, el propietario puede retirar la oferta ganadora (el monto más alto ofertado).

- onlyOwner: Solo el propietario del contrato puede llamar a esta función.
- onlyWhenEnded: Ejecutable solo al finalizar la subasta.
  Chequeos de seguridad:
  require(!fundsWithdrawn, "Funds already withdrawn"); Asegura que los fondos no hayan sido retirados previamente.
  require(highestBid > 0, "No funds to withdraw"); Permite el retiro solo si hay una oferta ganadora.
  Actualización del estado:
  fundsWithdrawn = true; Marca que los fondos ya fueron retirados.
  Transferencia de fondos:

(bool success,) = payable(owner).call{value: highestBid}(""); Envía el monto al propietario.

Verificación de la transferencia:
require(success, "Failed to withdraw funds"); Si la transferencia falla, la función revierte.

7. Consulta de Historial

Cualquier usuario puede consultar el número de ofertas y el historial completo de las mismas.

Variables Clave

owner: Dirección del propietario del contrato.

auctionEndTime: Momento en que finaliza la subasta.

maxExtensionTime y extendedTime: Controlan la extensión máxima de la subasta.

highestBidder y highestBid: Mejor postor y su oferta.

bidHistory: Historial de todas las ofertas.

deposits: Depósitos de cada usuario.

lastBid: Última oferta de cada usuario.

ended y fundsWithdrawn: Controlan el estado de la subasta y el retiro de fondos.

Consideraciones Adicionales

Uso de modificadores:
El contrato utiliza modificadores como onlyWhileActive, onlyWhenEnded, y onlyOwner para restringir el acceso y controlar el flujo de ejecución de las funciones. (visto en modulo 3)

Superar la mejor oferta en al menos 5%:
En la función bid, se exige que la nueva oferta sea al menos un 5% mayor que la oferta más alta actual:

Extensión automática de 10 minutos:
Si una oferta válida se realiza dentro de los últimos 10 minutos y no se ha excedido el máximo de extensión, la subasta se extiende automáticamente:

Seguridad y robustez:
El contrato maneja adecuadamente errores y situaciones excepcionales usando require para validar condiciones antes de ejecutar lógica crítica, y utiliza el patrón de retiro para transferencias de fondos

Eventos para cambios de estado:
Se emiten eventos como NewBid, AuctionEnded, PartialWithdrawal, DepositWithdrawn, AuctionCancelled, y FeeTransferred para notificar a los participantes sobre los cambios de estado.

Resumen

Este contrato permite realizar subastas seguras y transparentes, gestionando automáticamente las reglas de puja, extensiones de tiempo, depósitos y comisiones. Protege tanto a los ofertantes como al propietario, asegurando que los fondos se distribuyan correctamente según el resultado de la subasta.