

Subasta - Contrato Inteligente

Carlos Lagarón Real, Nicolas Araújo Calvar, Gonzalo Fernández Liberato

1. Análisis y Definición del Escenario

Este contrato es una subasta donde los usuarios pueden pujar con Ether por un producto o servicio ofrecido por un beneficiario. La subasta tiene las siguientes características:

- El contrato es desplegado por un beneficiario, que es quien recibe el dinero de la puja más alta cuando la subasta finaliza.
- El beneficiario puede establecer un tiempo límite para la subasta o dejarla indefinida.
- Los usuarios pueden realizar pujas, pudiendo ver el valor de la más alta.
- La subasta puede finalizar automáticamente cuando se alcanza el tiempo límite o ser cerrada manualmente por el beneficiario.
- Cuando se introduce una puja mayor, se devuelve el importe al pujador anterior.

El objetivo de este contrato es automatizar el proceso de subasta, eliminando la necesidad de un intermediario y garantizando que las reglas de la subasta se cumplan mediante la programación en la blockchain de Ethereum.

2. Diseño

2.1. Caso de Uso

El caso de uso es una subasta online, donde el beneficiario desea ofrecer un bien o servicio y los usuarios pujan por él. La lógica de negocio es la siguiente:

- Participantes:
 - **Beneficiario:** Persona que despliega el contrato y es quien recibirá el Ether de la subasta.
 - **Pujadores:** Usuarios que realizan pujas con Ether. El mayor pujador gana la subasta.

2.2. Variables y funciones

Variables:

- **beneficiario:** Dirección del beneficiario (dueño del contrato) que recibirá la mayor puja al final de la subasta.
- **finSubasta:** Tiempo de finalización de la subasta.
- **mayorPujador** y **mayorPuja:** Dirección del pujador que ha hecho la mayor puja y el valor de la puja.
- **finalizada:** Booleano que indica si la subasta ha finalizado.

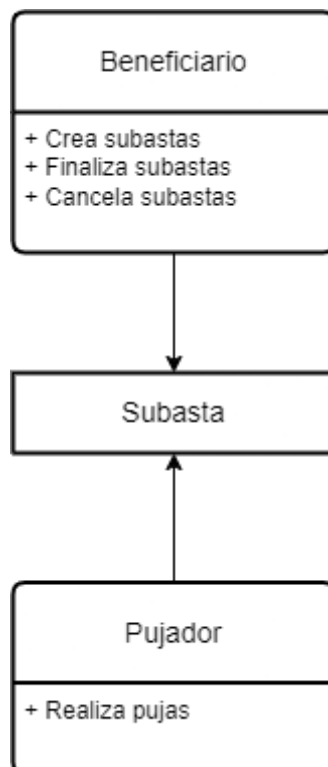
Funciones:

- `pujar()`: Permite a los usuarios realizar una puja.
- `finalizarSubasta()`: Permite al beneficiario cerrar la subasta y transferir los fondos.
- `cancelarSubasta()`: Cancela la subasta.
- `tiempoRestante()`: Devuelve el tiempo restante hasta que termine la subasta.
- `verificarFinAutomatico()`: Verifica si la subasta ha finalizado automáticamente.
- Funciones adicionales para consultar el beneficiario, la mayor puja y todas las pujas.

2.3. Usuarios del Sistema

- **Beneficiario**
 - Despliega el contrato.
 - Puede finalizar o cancelar la subasta.
 - Recibe los fondos si la subasta finaliza correctamente.
- **Pujadores**
 - Pueden realizar pujas en Ether.

Diagrama de Casos de Uso:



3. Implementación

El código del contrato está implementado en Solidity y tiene las siguientes funcionalidades clave:

- **Despliegue:** El constructor permite establecer un tiempo límite para la subasta. Si no se especifica, la subasta será indefinida.
- **Pujas:** Los usuarios pueden realizar pujas a través de la función `pujar()`, y si su puja es superada, se le devuelve el importe.
- **Finalización:** El beneficiario puede finalizar la subasta con la función `finalizarSubasta()` y recibir la mayor puja. La subasta se finaliza automáticamente al llegar al tiempo límite.
- **Cancelación:** Si el beneficiario cancela la subasta..
- **Consulta de datos:** Se pueden consultar los datos de la subasta (mayor puja, tiempo restante, etc.) a través de funciones de solo lectura.

4. Pruebas

El contrato fue probado en Remix IDE, donde se llevaron a cabo las siguientes pruebas:

- **Despliegue del contrato con tiempo limitado**
 - Se desplegó el contrato con un tiempo de subasta de 1 minuto y se ha comprobado que el tiempo restante en diferentes ocasiones.

```
[vm] from: 0x5B3...eddC4 to: Subasta.(constructor) value: 0 wei data: 0x608...00001 logs: 0 hash: 0x876...7dec0
status 0x1 Transaction mined and execution succeed Debug ^
```



```
decoded input {
  "uint256 _tiempoSubasta": "1"
}
```


```
call [call] from: 0x5B380a6a701c568545dCfcB03FcB875f56beddC4 to: Subasta.tiempoRestante() data: 0x4d2...793f8 Debug
from 0x5B380a6a701c568545dCfcB03FcB875f56beddC4
to Subasta.tiempoRestante() 0xEf9f1ACE83dfb88f5590a621f4aEA72C6EB10eBF
execution cost 2896 gas (Cost only applies when called by a contract)
input 0x4d2...793f8
output 0x0000000000000000000000000000000000000000000000000000000000000036
decoded input {}
decoded output {
  "0": "uint256: 54"
}
logs []
raw logs []
call to Subasta.tiempoRestante
```

```
CALL [call] from: 0x5838Da6a701c568545dcfc803Fc8875f56beddC4 to: Subasta.tiempoRestante() data: 0x4d2...793f8
from 0x5838Da6a701c568545dcfc803Fc8875f56beddC4
to Subasta.tiempoRestante() 0xEf9f1ACE83dfb88f5590a621f4aEA72C6E810eBf
execution cost 2896 gas (Cost only applies when called by a contract)
input 0x4d2...793f8
output 0x0000000000000000000000000000000000000000000000000000000000000011
decoded input {}
decoded output {"0": "uint256: 17"}
logs []
raw logs []
```

- **Realización de Pujas**

- Se ha realizado una puja al contrato anterior, como el tiempo se ha terminado salta un mensaje de error.

ACCOUNT +  



0xAb8...35cb2 (100 ether) 

GAS LIMIT

☒ Estimated Gas

☐ Custom 3000000

VALUE

5  Ether 

```
[vm] from: 0xAb8...35cb2 to: Subasta.pujar() 0xEf9...10e8f value: 500000000000000000 wei data: 0xe54...500e7 logs: 0 hash: 0xe34...a8189
transact to Subasta.pujar errored: Error occurred: revert.

revert
    The transaction has been reverted to the initial state.
    Reason provided by the contract: "La subasta ya ha finalizado".
    If the transaction failed for not having enough gas, try increasing the gas limit gently.
```

- Sobre un nuevo contrato, se han realizado pujas con distintas cuentas con valores de 5, 10 y 15 Ether respectivamente.

```
[vm] from: 0xAb8...35cb2 to: Subasta.pujar() 0x049...A1Fd3 value: 500000000000000000 wei data: 0xe54...500e7 logs: 1 hash: 0x95f...239ed
```

```
from 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
```

```
[vm] from: 0x4B2...C02db to: Subasta.pujar() 0x049...A1Fd3 value: 1000000000000000000 wei data: 0xe54...500e7 logs: 1 hash: 0xe4a...965c4
```

```
from 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
```

```
[vm] from: 0x787...cabaB to: Subasta.pujar() 0x049...A1Fd3 value: 1500000000000000000 wei data: 0xe54...500e7 logs: 1 hash: 0x0fd...ae080
```

0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB

- Se verificó que el `mayorPujador` y `mayorPuja` se actualizaban correctamente.

CALL

[call] from: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabAB to: Subasta.mayorPujador() data: 0x2c6...8d882

from 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabAB ⓘ

to Subasta.mayorPujador() @0x498B7c793D7432Cd9dB27fB02fc9cfdBFAf1Fd3 ⓘ

execution cost 2531 gas (Cost only applies when called by a contract) ⓘ

input 0x2c6...8d882 ⓘ

output 0x00000000000000000000000078731d3ca6b7e34ac0f824c42a7cc18a495cabab ⓘ

decoded input {} ⓘ

decoded output {
 "0": "address: 0x78731D3Ca6b7E34aC0F824c42a7CC18A495cabAB"
} ⓘ


logs [] ⓘ

raw logs [] ⓘ

```
call [call] from: 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB to: Subasta.mayorPuja() data: 0x74c...f6f75  
from 0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB  
to Subasta.mayorPuja() 0x049887c79307432cd9db27fb02fc9cfdbaFa1Fd3  
execution cost 2514 gas (Cost only applies when called by a contract)  
input 0x74c...f6f75  
output 0x0000000000000000000000000000000000000000000000000000000d02ab486cedc0000  
decoded input {}  
decoded output {  
    "0": "uint256: 15000000000000000000"  
}  
logs []  
raw logs []
```

- **Finalización de la Subasta**

- Se ha comprobado que el único usuario que puede terminar la subasta es el beneficiario.

 [vm] from: 0x787...cabaB to: Subasta.finalizarSubasta() 0x049...A1Fd3 value: 0 wei data: 0x085...1eac2 logs: 0 hash: 0x3e8...17af2
transact to Subasta.finalizarSubasta errored: Error occurred: revert.

revert

The transaction has been reverted to the initial state.
Reason provided by the contract: "Solo el beneficiario puede ejecutar esta funcion".
If the transaction failed for not having enough gas, try increasing the gas limit gently.

✓ [vm] from: 0x5B3...eddC4 to: Subasta.finalizarSubasta() 0x049...A1Fd3 value: 0 wei data: 0x085...1eac2 logs: 1 hash: 0xc7f...8e850 [Debug](#)

- El beneficiario finalizó la subasta correctamente y se transfirió la mayor puja a su cuenta.

0x5B3...eddC4 (114.999999999997382166 ether)