

Donación en Smart Contract

Juan Vila Luelmo

seguridad.usal.es



VNIVERSIDAD
DSALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL





Realización del Smart Contract

Idea

En mi caso he realizado un Smart Contract para realizar donaciones a nuestro billetero de **Ethereum**.

Esta donación estaría orientada, por ejemplo, a desarrolladores de cualquier tipo de contenido, a organizaciones recaudadoras de fondos para causas mayores como puede ser un desastre natural o a cualquier tipo de situación que necesite recaudar fondos en la plataforma ethereum.

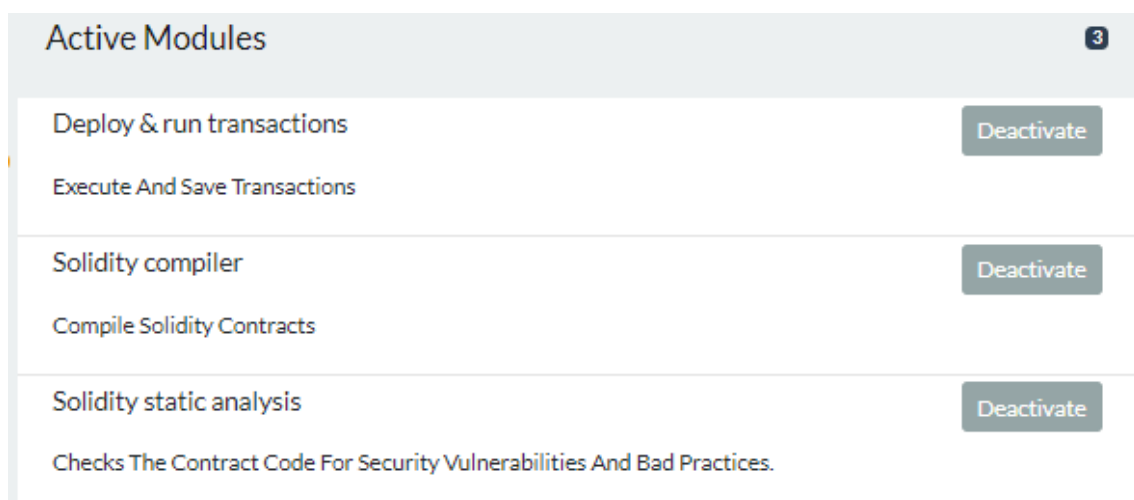
La donación mínima será de **1 ether**.

Si el donante introdujera una cantidad mayor a **3 ether** se le recompensará con un premio que no ha sido establecido, podría tratarse de una suscripción privilegiada o de cualquier tipo de obsequio que la propia organización pueda enviar hasta el donante.

Si el donante introduce una cantidad inferior a la donación mínima nuestra función para donar lanzaría un error.

Instalación de plugins en Remix

Para realizar esta práctica no he necesitado más que el compilador de **Solidity** proporcionado por Remix, el plugin “Deploy & run transactions” para que después de haber compilado el código podamos desplegar nuestro Smart Contract y el plugin “Solidity static analysis” para obtener información del funcionamiento del Smart Contract:





Obtención de GAS

Ahora comentaré el uso de GAS que tienen mis funciones en el contrato:

El mero hecho de desplegar el Smart Contract supone un gasto en ether de 0.000715, es decir, 715306 gas.

Abajo muestro el consumo de gas para nuestra cuenta de **metamask** y los detalles del despliegue del contrato donde aparecen las unidades en **gas**:

Transacción metamask:

DESPLEGAR (DEPLOY) CONTRATO

0

DETAILS DATA

EDIT

GAS FEE 0.000715
No hay tasa de conversión

AMOUNT + GAS FEE

TOTAL 0.000715
No hay tasa de conversión

Detalles del despliegue de nuestro contrato:

creation of Donacion pending...



[block: txIndex:] from:0xe54...62cb5 to:Donacion.(constructor) value:0 wei data:0x608...c0032 logs:0 hash:0xb74...a0941

status	0x1 Transaction mined and execution succeed
transaction hash	0xb74f31a553e0701255734f7e3fe318f74185e2a2c1cc1019c3ecdd96f6ea0941
from	0xe54589f634c6de4ef04fe17d5d6cef85f2d62cb5
to	Donacion.(constructor)
gas	715306 gas
transaction cost	715306 gas
hash	0xb74f31a553e0701255734f7e3fe318f74185e2a2c1cc1019c3ecdd96f6ea0941
input	0x608...c0032
decoded input	{ }
decoded output	-
logs	[]
value	0 wei



Llamar a nuestra función **donar** y pasarle los tres parámetros supondrá un coste de 159905 gas.

Detalles de llamar a la función donación y realizar el pago:

status	0x1 Transaction mined and execution succeed
transaction hash	0x433639b2990ad0c0e34bf92cbcd2a4a2a42cd874d082192a4c8ee784f938512a
from	0xe54589f634c6de4ef04fe17d5d6cef85f2d62cb5
to	Donacion.donar(uint8,string,string) 0xd9fce4a6f13da3fd0cb2c34538b88d175e49c7dc
gas	161387 gas
transaction cost	159905 gas
hash	0x433639b2990ad0c0e34bf92cbcd2a4a2a42cd874d082192a4c8ee784f938512a
input	0x467...00000
decoded input	{ "uint8 _dinero": 3, "string _nombre": "Juan Vila Luelmo", "string _motivo": "Donación para la causa" }
decoded output	-
logs	[{ "from": "0xd9fce4a6f13da3fd0cb2c34538b88d175e49c7dc", "topic": "0x8d85238c7381adcfcd8dca5d216ced114253b96cd225be0ccd7b2efa06e968a0", "event": "premio2", "args": { "0": true, "length": 1 } }, { "from": "0xd9fce4a6f13da3fd0cb2c34538b88d175e49c7dc", "topic": "0x93c156613cff8117d66f452356d65d3e0b61dd652e01b928d2f914997aeb54be", "event": "donado", "args": { "0": false, "length": 1 } }]
value	3000000000000000000 wei

El consultar las variables públicas **numdonaciones**, **premio** y **wallet** de nuestro contrato no supondrá ningún coste ya que no se realiza ningún computo en la red.



Detalles del pago de 3 ether mediante la llamada a la función donar:



Interacción Con Contrato
#19 - 1/19/2020 at 11:04

CONFIRMADO

-3 ETH

Detalles



De: 0xe54589F634C6De4ef04FE17d5d6cef85f2D62cB5

>

Para: 0xd9fCE4A6F13da3fD0cb2c34538B88d175E49c7dC

Transacción	
Cantidad	3 ETH
Límite De Gas (Unidades)	161387
Gas Usado (Unidades)	159905
Precio del Gas (GWEI)	1
Total	3.00016 ETH

Registro De Actividades



Se creó una transacción con un valor de 3 ETH, a 11:04 on 1/19/2020.



Se propuso la transacción con una comisión de gas de 0 WEI, en 11:04 on 1/19/2020.



Se confirmó la transacción a 11:04 on 1/19/2020.

Los comentarios acerca del funcionamiento del código se encuentran en donacion.sol que está adjuntado a este documento.