

Desarrollo Blockchain Ethereum con Solidity

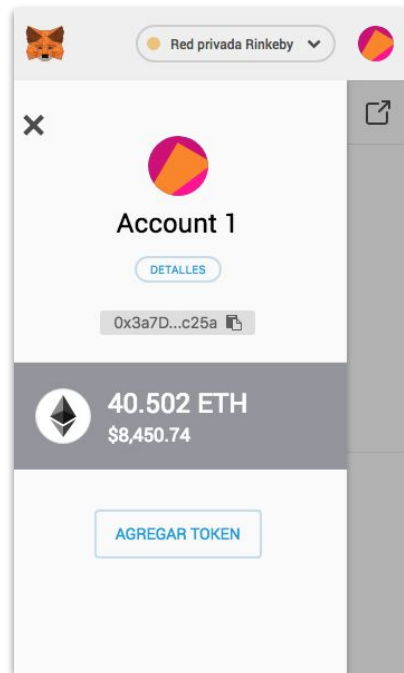
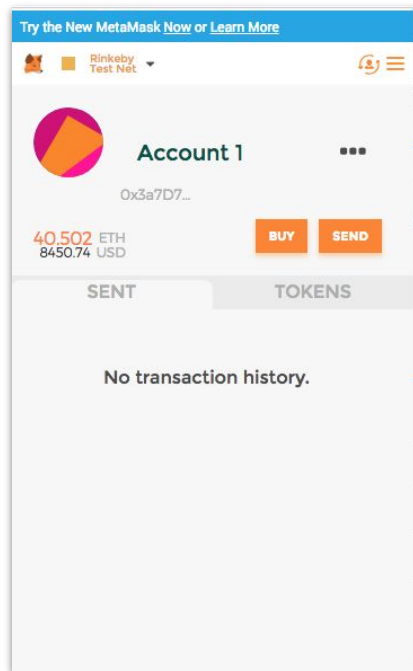
Módulo 1 – Enviando / Recibiendo Ether

Enviando / Recibiendo Ether

Enviando / Recibiendo Ether

Metamask posee dos interfaces para su utilización. Actualmente, la de la izquierda es la estable y la de la derecha es la BETA.

En cualquiera de las dos basta con presionar el botón "SEND" para enviar Ether a una dirección dentro de la Ethereum Blockchain.




Enviando / Recibiendo Ether

Al presionar SEND, se nos pedirá una dirección de envío (que puede ser cargada o escaneada por QR) y una cantidad de Ether a enviar.

Enviar Ether

Sólo envía a una dirección de Ethereum


De::

 Account 1

113.431895 ETH

\$24,846.12 USD

Para:

0x98d1F051B6c7b2Afc3F0c 

Cantidad:

1.4 ETH


Max

\$306.66 USD

Comisión de gas:

0.000021 ETH

\$0.00 USD



CANCELAR

SIGUIENTE


Enviando / Recibiendo Ether

Al presionar SEND, se nos pedirá una dirección de envío (que puede ser cargada o escaneada por QR) y una cantidad de Ether a enviar.

Enviar Ether

Sólo envía a una dirección de Ethereum


De::

 Account 1

113.431895 ETH

\$24,846.12 USD

Para:

0x98d1F051B6c7b2Afc3F0c 

Cantidad:

1.4 ETH


Max

\$306.66 USD

Comisión de gas:

0.000021 ETH

\$0.00 USD



CANCELAR

SIGUIENTE

Ejercicio

Solicitar Ethers de prueba en Ropsten Faucet:

<https://faucet.ropsten.be/>

Cada alumno deberá realizarle una transferencia al alumno que tenga inmediatamente debajo en la lista. Para eso, intercambiaremos las direcciones que nos muestra Metamask.

Discutir: *¿Qué pasó con los saldos?*



GAS

- El GAS podemos decir que es el precio de las transacciones en los contratos de Ethereum.
- Para hacer una analogía, sería como los KiloWatts para contar el gasto de electricidad. Es el costo por ejecutar algo.
- En teoría, el GAS sirve para desacoplar el precio del Ether al de la ejecución de contratos dado que el GAS tiene de por sí, un precio en Ether.
- El mismo dependerá de las operaciones que ejecute.
- Al ejecutar una transacción sobre un contratos, fijaremos el precio GAS que estamos dispuestos a pagar, cuanto más gas, mayor será la prioridad de nuestra transacción en la blockchain ya que los mineros tomarán primero las transacciones más lucrativas.
- Supongamos que crear un contrato cuesta hoy unos 32000 GAS. Si le ponemos un precio de 25 gwei tenemos que la transacción nos costará 0.008 ETH ($32000 * 25 / 10^8$)

GAS








Existe un documento público donde se indica el costo de GAS según las operaciones realizadas. El mismo se encuentra en:

https://docs.google.com/spreadsheets/d/1n6mRqkBz3iWcOlRem_mO09GtSKEKrAsfO7Frgx18pNU/edit#gid=0

Gas Costs from Yellow Paper – EIP-150 Revision (1e18248 - 2017-04-12)													
Archivo Editar Ver Insertar Formato Datos Herramientas Complementos Ayuda													
Solo ver													
Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes	Formula	Formula Notes					
0x00	STOP	0	zero	0	0	Halts execution.							
0x01	ADD	3	verylow	2	1	Addition operation.							
0x02	MUL	5	low	2	1	Multiplication operation.							
0x03	SUB	3	verylow	2	1	Subtraction operation.							
0x04	DIV	5	low	2	1	Integer division operation.							
0x05	SDIV	5	low	2	1	Signed integer division operation (truncated).							
0x06	MOD	5	low	2	1	Modulo remainder operation.							
0x07	SMOD	5	low	2	1	Signed modulo remainder operation.							
0x08	ADDMOD	8	mid	3	1	Modulo addition operation.							
0x09	MULMOD	8	mid	3	1	Modulo multiplication operation.							
0x0a	EXP	FORMULA		2	1	Exponential operation.	(exp == 0) ? 10 :	If exponent is 0, gas used is 10. If exponent is greater than 0, gas used is 10 plus 10 times a factor related to how large the log of the expo					
0x0b	SIGNEXTEND	5	low	2	1	Extend length of two's complement signed integer.							
0x10	LT	3	verylow	2	1	Less-than comparison.							
0x11	GT	3	verylow	2	1	Greater-than comparison.							
0x12	SLT	3	verylow	2	1	Signed less-than comparison.							
0x13	SGT	3	verylow	2	1	Signed greater-than comparison.							
0x14	EQ	3	verylow	2	1	Equality comparison.							
0x15	ISZERO	3	verylow	1	1	Simple not operator.							
0x16	AND	3	verylow	2	1	Bitwise AND operation.							
0x17	OR	3	verylow	2	1	Bitwise OR operation.							
0x18	XOR	3	verylow	2	1	Bitwise XOR operation.							
0x19	NOT	3	verylow	1	1	Bitwise NOT operation.							
0x1a	BYTE	3	verylow	2	1	Retrieve single byte from word.							

Transacciones

Una transacción es un registro de una operación realizada sobre la blockchain.

Transaction Hash:	0x28fe5de393ac3d79db9d7ab9e672d64dda96e60651c36e9e155dc4224cf04518 
Status:	 Success
Block:	12433399  2 Block Confirmations
Timestamp:	⌚ 39 secs ago (May-14-2021 03:48:59 PM +UTC) ⌚ Confirmed within 3 secs
From:	0xe102dd3261acf283d217d8658d8f1bf0f7da3d60 
To:	0x42af4214aaf3d824dfe16acd41f4dc0ece79cfa3 
Value:	0.06089169802589115 Ether (\$250.41)
Transaction Fee:	0.004158 Ether (\$17.10)
Gas Price:	0.000000198 Ether (198 Gwei)
Gas Limit:	21,000
Gas Used by Transaction:	21,000 (100%)
Nonce  Position	5  237
Input Data:	0x

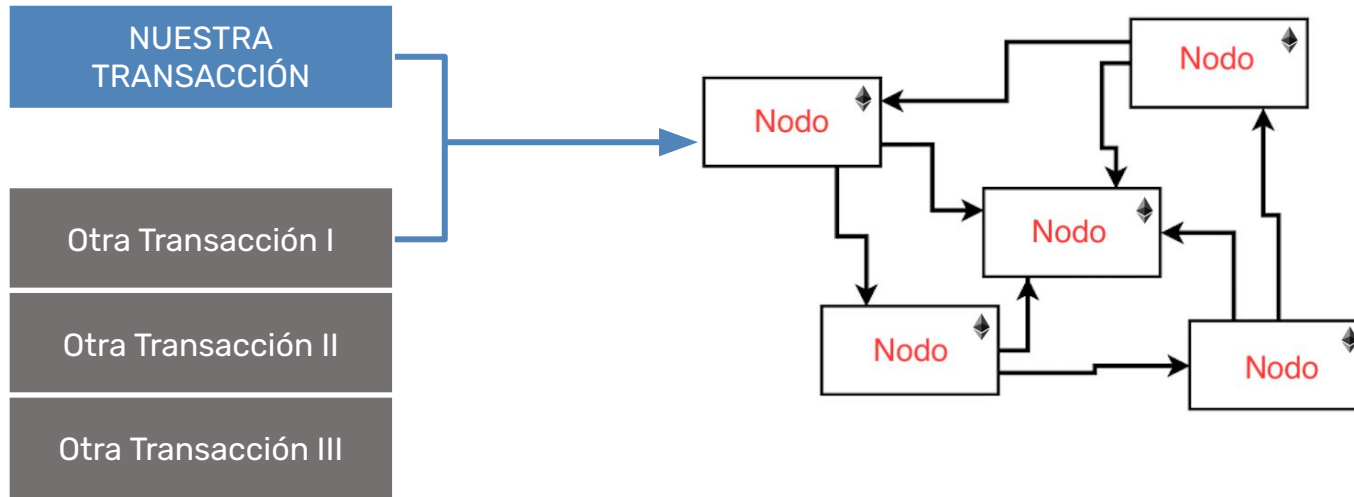
Transacciones

Toda transacción tiene múltiples propiedades. Entre las más importantes, se encuentran las siguientes:

Nonce	Cuántas veces el sender(remitente) ha enviado una transacción.
To	Address a donde estará llegando el Ether enviado.
Value	Cantidad de Ether que se está enviando al "To".
gasPrice	Cantidad de Ether que quien envía está esperando pagar por unidad de GAS para que esta transacción sea procesada.
startGas / gasLimit	Unidades de gas que la transacción puede consumir.
v	Parte criptográfica de información que puede ser utilizada para generar la dirección (Address) de quien envía el Ether.
r	Idem anterior.
s	Idem anterior.

Transacciones

Es importante aclarar que cuando enviamos una transacción a la blockchain, en realidad la estaremos enviando a un nodo particular y no al conjunto (EN)



Transaction Hash

Cuando realizamos una transacción obtendremos un hash asociado al mismo. Recibir este Hash no implica que la transacción se haya confirmado, sólo nos indica que se envió correctamente, pero puede que al llegar al nodo no se pueda realizar por algún motivo y se descarte. Por ejemplo, si el saldo de mi cuenta ya se gastó en otra transacción.

Para ver el estado de una transacción podemos buscar en el explorer por medio del hash y ver si nuestra transacción fue exitosa.

Transaction Details

Overview

State

Comments

? Transaction Hash:

0xfa332ad76cc3c57a2cce1d3c5019c4f4e81df4353c2c201397f6daa5d0785caf 

? Status:

 Success

¡Muchas gracias!

¡Sigamos trabajando!