



# **ETHEREUM SMART CONTRACT DEMO**

## **Aryan Nava Token(ARN)**

**The official token symbol for Aryan Nava Token : ARN**

**Token Type: ERC20**

**Decimals allowed : 18**

**ARN Coinig Total Supply : 200,000,000**

**Price : 1ETH = 100ARN Tokens**

# Deployment and Testing of Ethereum Smart Contract

**Method:** MetaMask Plugin

**Platform:** Remix.ethereum.org

**Test setup:** Rinkeby Test Network

## **Process:**

**Step 1:** Browse <https://remix.ethereum.org/> click on the top left button “+” a new file will be created enter the new file name as shown below





File Name

Untitled.sol

OK Cancel

**Step 2:** Copy the code solidity code from file :“ ARN\_Crowdsale.sol ” and paste it in <https://remix.ethereum.org> as shown below.

Under the Compile tab, click on start to compile to successfully complete the compilation process as shown below.

```
1 pragma solidity ^0.4.24;
2
3 /**
4  * @title SafeMath
5  * @dev Math operations with safety checks that revert on error
6  */
7 library SafeMath {
8
9     /**
10     * @dev Multiplies two numbers, reverts on overflow.
11     */
12     function mul(uint256 _a, uint256 _b) internal pure returns (uint256) {
13         // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
14         // benefit is lost if 'b' is also tested.
15         // See: https://github.com/OpenZeppelin/openzeppelin-solidity/pull/522
16         if (_a == 0) {
17             return 0;
18         }
19         uint256 c = _a * _b;
20         require(c / _a == _b);
21         return c;
22     }
23 }
24
25
```

Compile Run Settings Analysis Debugger Support

Start to compile Auto compile

AryanNavaCro Details Publish on Swarm

[2] only remix transactions, script Search transactions



**Step 3:** Click on Run and set Environment and account address as shown in the image below.

The screenshot displays the Remix IDE interface with the following details:

- File Explorer:** Shows 'browser' and 'config' folders.
- Editor:** Contains a Solidity contract named 'ARN\_Crowdsale.sol' with the following code:

```
1 pragma solidity ^0.4.24;
2
3 /**
4  * @title SafeMath
5  * @dev Math operations with safety checks that revert on error
6  */
7 library SafeMath {
8
9     /**
10    * @dev Multiplies two numbers, reverts on overflow.
11    */
12    function mul(uint256 _a, uint256 _b) internal pure returns (uint256) {
13        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
14        // benefit is lost if 'b' is also tested.
15        // See: https://github.com/OpenZeppelin/openzeppelin-solidity/pull/522
16        if (_a == 0) {
17            return 0;
18        }
19
20        uint256 c = _a * _b;
21        require(c / _a == _b);
22
23        return c;
24    }
25 }
```
- Run Tab:** Contains deployment settings:
  - Environment:** Injected Web3 (Rinkeby (4))
  - Account:** 0x796...84d65 (4.076915166 ether)
  - Gas limit:** 3000000
  - Value:** 0 wei
  - Contract Name:** AryanNavaCrowdsale
  - Deploy Button:** Highlighted in red.
  - Load contract from Address:** At Address
  - Transactions recorded:** 0
  - Deployed Contracts:** Currently you have no contract instances to interact with.
- Footer:** Shows '[2] only remix transactions, script' and a search bar for transactions.

Make sure that the Wallet address in Metamask and remix IDE is same while deploying a Contract as shown below



Environment: Injected Web3 Rinkeby (4) i

Account: 0x796...84d65 (4.076915166 ether) v

Gas limit: 3000000

Value: 0 wei v



Rinkeby Test Net

Account 1

0x796c3...

4.076 ETH  
941.97 USD

BUY SEND

**Step 4:** Click on Deploy button under the Run tab and click on the submit tab in the new popup transaction window, so contract is started to deploy

browser/ARN\_Crowdsale.sol

MetaMask Notification

CONFIRM TRANSACTION

Account 1  
796c35...4D65  
4.076 ETH  
933.41 USD

New Contract

Amount: 0 ETH  
0.00 USD

Gas Limit: 4276941 UNITS

Gas Price: 51 GWEI

Max Transaction Fee: 0.218123 ETH  
49.94 USD

Max Total: 0.218123 ETH  
49.94 USD

Data Included: 15267 bytes

RESET SUBMIT REJECT

Compile Run Settings Analysis Debugger Support

Environment: Injected Web3 Rinkeby (4) i

Account: 0x796...84d65 (4.076915166 ether) v

Gas limit: 3000000

Value: 0 wei v

AryanNavaCrowdsale

Deploy

Load contract from Address At Address

Transactions recorded: 1

Deployed Contracts

Currently you have no contract instances to interact with.



**Step 5:** Once the contract is Deployed , a list of contract functionalities in the right bottom corner as shown below.

AryanNavaCrowdsale at 0xf95...3deb4  
(blockchain)

(fallback)

buyTokens

address\_beneficiary

claimRefund

address\_beneficiary

finalize

renounceOwnership

transferOwnership

address\_newOwner

cap

capReached

closingTime

goal

goalReached

hasClosed

isFinalized

openingTime

owner

rate

token

wallet

weiRaised

address\_newOv



**Step 6:** To Confirm the Transaction is successful click on the rinkeby.etherscan.io link which will redirect to a etherscan page as shown below

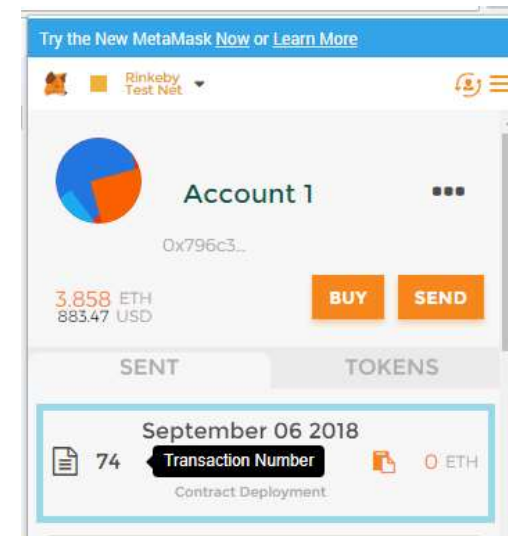
```
1 pragma solidity ^0.4.24;
2
3 /**
4  * @title SafeMath
5  * @dev Math operations with safety checks that revert on error
6  */
7 library SafeMath {
8
9     /**
10     * @dev Multiplies two numbers, reverts on overflow.
11     */
12     function mul(uint256 _a, uint256 _b) internal pure returns (uint256) {
13         // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
14         // benefit is lost if 'b' is also tested.
15         // See: https://github.com/OpenZeppelin/openzeppelin-solidity/pull/522
16         if (_a == 0) {
17             return 0;
18         }
19
20         uint256 c = _a * _b;
21         require(c / _a == _b);
22
23         return c;
24     }
25 }
```

creation of AryanNavaCrowdsale pending...

<https://rinkeby.etherscan.io/tx/0xdfbc03e1906c95af4a7d9dfdb29d49dc372350f1a4cdaa89109dc658db5e9f38>

[block:2941834 txIndex:0] from:0x796...84d65 to:AryanNavaCrowdsale.(constructor) value:0 wei data:0x608...a0029 logs:0 hash:0xdfb...e9f38

(OR)





Transaction Hash ,Transaction Status, Contract Address, Gas Price are displayed as shown below

Secure | <https://rinkeby.etherscan.io/tx/0xdfbc03e1906c95af4a7d9fdb29d49dc372350f1a4cdaa89109dc658db5e9f38> ☆

Transaction 0xdfbc03e1906c95af4a7d9fdb29d49dc372350f1a4cdaa89109dc658db5e9f38 Home / Transactions / Tx Info

Overview Internal Transactions

Transaction Information Tools & Utilities

[ This is a Rinkeby Testnet Transaction Only ]

TxHash:	0xdfbc03e1906c95af4a7d9fdb29d49dc372350f1a4cdaa89109dc658db5e9f38
TxReceipt Status:	Success
Block Height:	2941834 (2 block confirmations)
TimeStamp:	35 secs ago (Sep-06-2018 03:06:59 PM +UTC)
From:	0x796c35f4fb6270daf566043ef85c97e7f5184d65
To:	[Contract 0xf95b26851f0402d1b8c98803eea080928d13deb4 Created] ✓
Value:	0 Ether (\$0.00)
Gas Limit:	4276941
Gas Used By Txn:	4276941
Gas Price:	0.000000051 Ether (51 Gwei)
Actual Tx Cost/Fee:	0.218123991 Ether (\$0.000000)
Nonce & {Position}:	74   {0}
Input Data:	



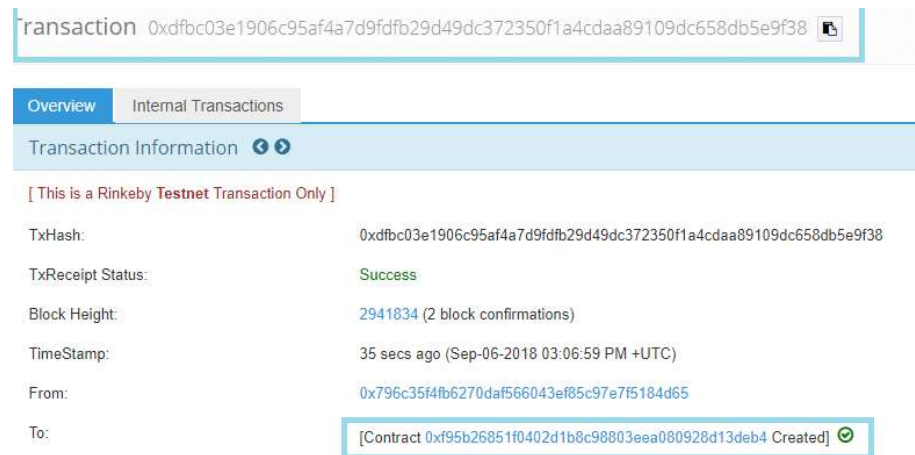
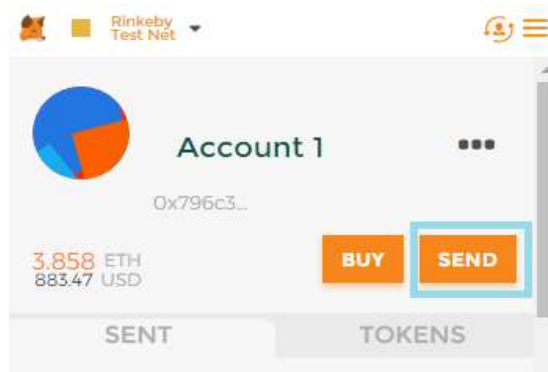


## Test Scenarios to Buy Tokens:



### 1. Transferring Ethers from wallet Account (address) to owner account(contract Account).



**Step 1:** Browse to Account 1 and click on the **SEND** button to send some Ethers to Owner Account.

**Step 2:** Enter the **Contract address** , Enter the number of Ethers to send and click on **NEXT** button which will redirect to Transaction Confirmation window click on **SUBMIT** button .





Rinkeby Test Net





**Account 1**  
0x796c35F4...4D65  
3.858 ETH  
883.47 USD


SEND TRANSACTION



NEXT

TRANSACTION DATA (OPTIONAL)



Rinkeby Test Net

**CONFIRM TRANSACTION**

**Account 1**  
796c35...4D65  >  F95B26...DEB4  
3.858 ETH  
878.69 USD

Amount 1.000 ETH  
227.71 USD

Gas Limit  UNITS

Gas Price  GWEI

Max Transaction Fee 0.000186 ETH  
0.04 USD

Max Total 1.000 ETH  
227.75 USD

Data included: 0 bytes

RESET

SUBMIT

REJECT



**Step 3:** Once the transaction is successful, To confirm browse to [rinkeby.etherscan.io](https://rinkeby.etherscan.io) and check the Transaction Status.

To view the ERC20 Token Contract address click on the ERC20(ARN) will redirect to a ERC20 Token Page as shown below

**Transaction** 0x3aa1358e66689d1bab8d8a1e6bca784a262fae56fefa269fccabaf13c28bc5a

Home / Transactions / Tx Info

OverviewInternal TransactionsEvent Logs (4)

Transaction Information

Tools & Utilities

[ This is a Rinkeby **Testnet** Transaction Only ]

TxHash:

0x3aa1358e66689d1bab8d8a1e6bca784a262fae56fefa269fccabaf13c28bc5a

TxReceipt Status:

Success

Block Height:

2941878 (5 block confirmations)

TimeStamp:

1 min ago (Sep-06-2018 03:17:59 PM +UTC)

From:

0x796c35f4fb6270daf566043ef85c97e7f5184d65

To:

Contract 0xf95b26851f0402d1b8c98803eea080928d13deb4

TRANSFER 1 Ether from 0xf95b26851f0402d1b8c98... to 0x528c81a4d7d5c0ae56a8...

Token Transferred:

From 0x0000000000000000... To 0x796c35f4fb6270d... for 100 ERC20 (ARN)

Value:

1 Ether (\$0.00)

Gas Limit:

95944

Gas Used By Txn:

63963

Gas Price:


0.000000061 Ether (61 Gwei)

Actual Tx Cost/Fee:

0.003901743 Ether (\$0.000000)







RINKEBY (CLIQUE) TESTNET

Search by Address / Txhash / Block / Token / Ens

GO

HOMEBLOCKCHAIN ▼TOKEN ▼MISC ▼

Token AryanNava Token

Home / ERC-20 TokenTracker / AryanNava Token

Summary [ERC-20]

Total Supply: 200 ARN

Holders: 1 addresses

Transfers: 2

Contract: 0x6b27f3b40fce83f86c0ac8034e19543d353b4575

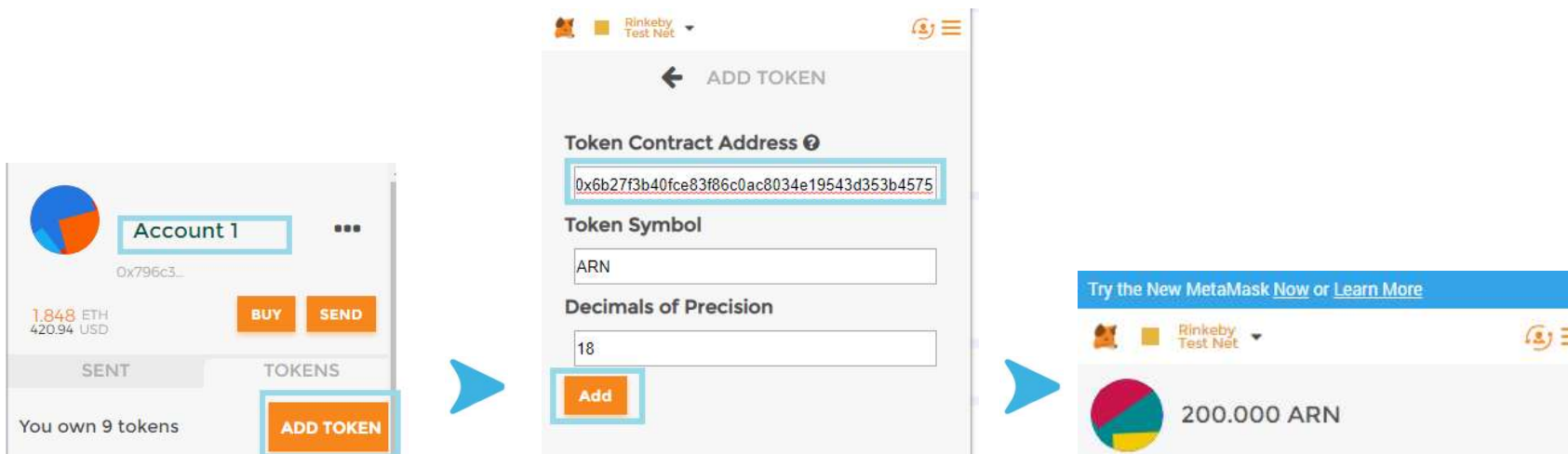
Decimals: 18

Links: Not Available, [Update ?](#)

Filtered By: 

Apply

**Step 5:** To view the Tokens Browse to Metamask and select **Account 1 Wallet** Click on **ADD TOKEN** which will redirect to add another tab Enter the **contract address**(Contract address is ERC20 Token address as shown above image) ,Automatically Token symbol will be replaced with “**ARN**” and click on **Add** button then the number of Tokens are present in Account 1 are displayed. Refer below diagrams





## Note : Other Functionalities of ICO

cap	
	0: uint256: 20000000000000000000
capReached	
closingTime	
goal	
	0: uint256: 10000000000000000000
goalReached	
hasClosed	
isFinalized	
openingTime	
owner	
	0: address: 0x796c35F4fB6270Daf566043ef85C97e7f5184D65
rate	
	0: uint256: 100
token	
	0: address: 0x6b27f3B40fCe83f86C0aC8034E19543d353B4575
wallet	
	0: address: 0x796c35F4fB6270Daf566043ef85C97e7f5184D65