UNIVERSITY OF THESSALY
SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL
& COMPUTER ENGINEERING

Project: Develop and Deploy a Smart Contract

Μάθημα: Τεχνολογίες blockchain και αποκεντρωμένες εφαρμογές

Διδάσκων: ΦΩΤΗ ΜΑΓΔΑΛΗΝΗ

Ακ. έτος 2020-21, εαρινό εξάμηνο

Ονοματεπώνυμο: Καραμούστου Βασιλική

ΑΕΜ: 02424

Contents

Προετοιμάστε τρεις λογαριασμούς για τον έλεγχο του smart contact.

>./geth --identity "Node 1" --datadir node1 --nat "extip:127.0.0.1" --port 50001 -nodiscover -- networkid 1000 --http --http.port 51001 --http.api "eth,net,web3,miner,admin,personal" -- http.corsdomain "*" --allow-insecure-unlock

>./geth attach http://localhost:51001

>web3.personal.unlockAccount(eth.accounts[0],"5555",1000000)

>personal.newAccount()

>web3.personal.unlockAccount(eth.accounts[1],"5555",1000000)

>personal.newAccount()

>web3.personal.unlockAccount(eth.accounts[2],"5555",1000000)

Ολοκληρώστε την υλοποίηση του smart contract και αποθηκεύστε το ως "Auction.sol".

Ο κώδικας για την υλοποίηση του smart contract παρατίθεται σε αρχείο με όνομα **auction**.txt.

Κάνετε compile τον κώδικα.

>solc --abi auction.sol

[{"inputs":[],"stateMutability":"nonpayable","type":"constructor"},{"inputs":[],"name":"auction_finished","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"bid","outputs":[],"stateMutability":"payable","type":"function","payable":true},{"inputs":[],"name":"canWithdraw","outputs":[{"internalType":"bool","name":"","type":"bool"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"finish_auction","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":[{"internalType":"address","name":"_bidder","type":"address"}],"name":"getBidderBalance","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"getContractBalance","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"highestBid","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"highestBidder","outputs":[{"internalType":"address","name":"","type":"address"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"","type":"address"}],"name":"userBalances","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"withdraw","outputs":[],"stateMutability":"payable","type":"function","payable":true},{"stateMutability":"payable","type":"receive"}]

>solc --bin auction.sol

60806040526000600455348015610015576000 80fd5b50336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550600060038190555060006002819055506000805490610100 0a900473ffffffffffffffffffffffffffffffffffffffff1660016000610100 0a81548173ffffffffffffffffffffffffffffffffffffffff02191690837 3ffffffffffffffffffffffffffffffffffffffff16021790555061 0cbc806100d66000396000f3fe6080604052600436106100555760003560e01c80631998aeef1461005a57806326224c64146100645780633ccfd60b146100a15780636f9fb98a146100b857806391f90157146100e3578063d57bde791461010e575b600080fd5b610062610139565b005b348015610070576000 80fd5b5061008b600480360381019061008691906108395 65b6104bc565b604051610098 9190610a2d565b60405180910390f35b3480156100ad57600080fd5b506100b66104d45 65b005b3480156100c457600080fd5b506100cd6107f0565b6040516100da9190610a2d5 65b60405180910390f35b3480156100ef57600080fd5b506100f86107f8565b6040516101

059190610952565b60405180910390f35b34801561011a57600080fd5b5061012361081
e565b604051610130919061 0a2d565b60405180910390f35b6000805490610100 0a9004
73ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffff
ffffffffffffffffffff1614156101c8576040517f08c379a0000000000000000000000000000000
0000000000000000000000000000815260040161 01bf906109cd565b60405180910390f
d5b600254341161020c576040517f08c379a0000000000000000000000000000000000000
0000000000000000000000815260040161 0203906109ad565b60405180910390fd5b600
2546005819055506001600090549061 01000a900473ffffffffffffffffffffffffffffffffffffffff166
00660006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffff
ffffffffffffffffff160217905550346002819055503360016000 6101000a81548173ffffffffff
ffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506007
60003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff1681526020
019081526020016000205434111561047657600600760003373ffffffffffffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020541461 0
475573373ffffffffffffffffffffffffffffffffffffffff166108fc600760003373ffffffffffffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020549081
150290604051600060405180830381858888f193505050506104745760055460028190 5
55060066000905490 6101000a900473ffffffffffffffffffffffffffffffffffffffff166001600061010
00a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff
f160217905550600161047357 6040517f08c379a0000000000000000000000000000000
0000000000000000000000000815260040161046a906109ed565b60405180910390fd5
b5b5b5b34600760003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff
ffff168152602001908152602001600020819055505 65b60076020528060005260406000
206000915090505481565b60016000905490 6101000a900473ffffffffffffffffffffffffffffffffffffffff
fffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff161415610
565576040517f08c379a0000000000000000000000000000000000000000000000000000000
0000008152600401610 55c9061098d565b60405180910390fd5b600600760003373fffff
ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602
00160002054118061 05fe57506000805490 6101000a900473ffffffffffffffffffffffffffffffffffffffff
fff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff16145b61063
d576040517f08c379a0000000000000000000000000000000000000000000000000000000
0000815260040161063490610 96d565b60405180910390fd5b600080549061010 00a900
473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffff
ffffffffffffffffffff16141561069f576002546004819055506107 2b565b600760003373ffff
ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602
00160002054600481905550600600760003373ffffffffffffffffffffffffffffffffffffffff1673ffffff
ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020819055505b3373ffffffffff
ffffffffffffffffffffffff166108fc60045490811502906040516000604051808303818588 8
8f193505050506107ee576004546007600033 73ffffffffffffffffffffffffffffffffffffffff1673fffffff
ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020819055506001 6107ed576
040517f08c379a0000000000000000000000000000000000000000000000000000000000000

81526004016107e490610a0d565b6040518091039 0fd5b5b565b600047905090565b600160009054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b60025481565b600081359050610833816 10c6f565b92915050565b60006020828403121561084b576000080fd5b60006108598482850161082456 5b91505092915050565b61086b81610a59565b82525050565b600061087e602f83610a48565b91506108898261 0a95565b604082019050919050565b60006108a1603583610a48565b91506108ac82610ae4565b6040820190509190505 65b60006108c4602683610a48565b91506108cf82610b33565b60408201905091905 0565b60006108e7602d83610a48565b91506108f282610b82565b604082019050919050565b600061090a602f83610a48565b9150610915 82610bd1565b6040820190509190505 65b600061092d603083610a48565b91506109388 2610c20565b60408201905091905 0565b61094c81610a8b565b82525050565b60006020820190506109760008301846108 62565b92915050565b60006020820190508181036000830152610986816108715 65b9050919050565b60006020820190508181036000830152610a9a816108945 65b9050919050565b60006020820190508181036000830152610ab3816108ad 565b9050919050565b60006020820190508181036000830152610acc816108c6 565b9050919050565b60006020820190508181036000830152610ae581610 8de565b9050919050565b60006020820190508181036000830152610afe816108f7 565b9050919050565b60006020820190508181036000830152610b17816109109 050565b60006020820190508181036000830152610b30816109295 65b9050919050565b60006020820190508181036000830152610b49816109429 050565b60006020820190508181036000830152610b62816109 5b565b9050919050565b60006020820190508181036000830152610b7b816109 73ffffffffffffffffffffffffffffffffffffffff8216905091905056 5b60008190509190505 65b7f54686520616d6f756e7420746f2072657475726e206d75737420626520677265600082015 27f6174657220746861 6e207a65726f2100000000000000000000000000000000602082015250565b7f596f752063616e206e6f74206265207468652068696768657374426964646572600082015 27f20696e206f7264657220746f2070726f6365564210000000000000000000000602082015250565b7f5468657265206973206 16c7265616479206120736 16d65206f722068696768656000820152 7f2206269642100000000000000000000000000000000000000000000000000000602082015250565b7f596f752063616e206e6f74206265207468652068696768657374426964646572600820152 7f2220746f2070726f6365564210000000000000000000000000000000000000006020820152 50565b7f596f752068616420616e20756e7375636365737366756c206361 6c6c206f662060008201527f6269742c207472792061676169 6e2100000000000000000000000000000000602082015250565b7f596f752068616420616e20756e737563636573736756c2063616c6c206f662060008201527f73656e642c207472792061676169 6e210000000000000000000000000000000602082015250565b610c7881610a59565b8114610c8357600 80fd5b5056fea2646970667358221220a6800788f15b76834dc8a30ddf320bbaac0d28e660e2fafb54c06b31a216dbdd64736f6c63430008030033

Αποστολή transaction για τη δημιουργία του smart contract, από τον λογαριασμό 1 (κάτοχος).

>var abi =
eth.contract([{"inputs":[],"stateMutability":"nonpayable","type":"constructor"},{"inputs":[],"name":"auction_finished","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"bid","outputs":[],"stateMutability":"payable","type":"function","payable":true},{"inputs":[],"name":"canWithdraw","outputs":[{"internalType":"bool","name":"","type":"bool"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"finish_auction","outputs":[],"stateMutability":"nonpayable","type":"function"},{"inputs":[{"internalType":"address","name":"_bidder","type":"address"}],"name":"getBidderBalance","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"getContractBalance","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"highestBid","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"highestBidder","outputs":[{"internalType":"address","name":"","type":"address"}],"stateMutability":"view","type":"function"},{"inputs":[{"internalType":"address","name":"","type":"address"}],"name":"userBalances","outputs":[{"internalType":"uint256","name":"","type":"uint256"}],"stateMutability":"view","type":"function"},{"inputs":[],"name":"withdraw","outputs":[],"stateMutability":"payable","type":"function","payable":true},{"stateMutability":"payable","type":"receive"}])

>var bytecode =
'0x6080604052600060045534801561001557600080fd5b5033600080610100a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550600060038190555060006002819055506000805490610100a900473ffffffffffffffffffffffffffffffffffffffff16600160006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550610cbc806100d66000396000f3fe6080604052600436106100555760003560e01c80631998aeef1461005a57806326224c64146100645780633ccfd60b146100a15780636f9fb98a146100b857806391f90157146100e3578063d57bde791461010e575b600080fd5b610062610139565b005b3480156100705760008fd5b5061008b600480360381019061008691906108395565b6104bc565b6040516100989190610a2d565b60405180910390f35b3480156100ad57600080fd5b506100b6610d4565b005b3480156100c457600080fd5b506100cd6107f0565b6040516100da9190610a2d565b60405180910390f35b3480156100ef57600080fd5b506100f861086107f8565b6040516101019190610952565b60405180910390f35b34801561011a57600080fd5b5061012361081e565b60405161013091906108a2565b60405180910390f35b60008054906101000

a900473ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffff163373ffffffff
ffffffffffffffffffffffffffff1614156101c8576040517f08c379a0000000000000000000000000
0000000000000000000000000000000008152600401610 1bf906109cd565b6040518091
0390fd5b60025434116102 0c576040517f08c379a0000000000000000000000000000000
0000000000000000000000000008152600401610203906109ad565b60405180910390fd5
b60025460058190555060016000905490610100 0a900473ffffffffffffffffffffffffffffffffffffff
f16600660006101000a81548173ffffffffffffffffffffffffffffffffffffff021916908373ffffffffffff
ffffffffffffffffffffffff160217905550346002819055503360016000610100 0a81548173ffff
ffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffff1602179055506
00760003373ffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffff1681526
020019081526020016000205434111561047657600060076000 3373ffffffffffffffffffffffff
ffffffffffff1673ffffffffffffffffffffffffffffffffffffff168152602001908152602001600020541 4
610475573373ffffffffffffffffffffffffffffffffffffff166108fc600760003373ffffffffffffffffffffff
ffffffffffff1673ffffffffffffffffffffffffffffffffffffff168152602001908152602001600020549
081150290604051600060405180830381858888f193505050506104745760055460028 1
905550600660009054906101000a900473ffffffffffffffffffffffffffffffffffffff166001600061
01000a81548173ffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffff
ffffff160217905550600161047357604051 7f08c379a0000000000000000000000000000
0000000000000000000000000008152600401610 46a906109ed565b60405180910390f
d5b5b5b5b34600760003373ffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffff
ffffffff168152602001908152602001600020819055505 65b600760205280600052604060
0020600091509050548 1565b600160009054906101000a900473ffffffffffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffff1614156
10565576040517f08c379a0000000000000000000000000000000000000000000000000000
0000000815260040161055c9061098d565b60405180910390fd5b6000600760003373ff
ffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffff168152602001908152602
0016000205411806105fe575060008054906101000a900473ffffffffffffffffffffffffffffffffffffff
ffff1673ffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffff16145b610
63d576040517f08c379a0000000000000000000000000000000000000000000000000000
0000008152600401610634906 1096d565b60405180910390fd5b60008054906101000a9
00473ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffff163373ffffffffffff
ffffffffffffffffffffffff16141561069f576002546004819055506 1072b565b600760003373f
ffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffff168152602001908152602
0016000205460048190555060006007600033 73ffffffffffffffffffffffffffffffffffffff1673fff
ffffffffffffffffffffffffffffffffff168152602001908152602001600020819055505b3373ffffffff
ffffffffffffffffffffffffffff166108fc600454908115029060405160006040518083038185 8
888f193505050506107ee576004546007600033 73ffffffffffffffffffffffffffffffffffffff1673fff
ffffffffffffffffffffffffffffffffff168152602001908152602001600020819055506001610 7ed
576040517f08c379a0000000000000000000000000000000000000000000000000000000000
0008152600401610 7e490610a0d565b60405180910390fd5b5b565b600047905090565b
60016000905490610100 0a900473ffffffffffffffffffffffffffffffffffffff1681565b6002548156

5b60008135905061083381610c6f565b92915050565b60006020828403121561084b576
00080fd5b60006108598482850161082456 5b9150509291505056 5b61086b81610a5956
5b82525050565b600061087e602f83610a48565b915061088982610a95565b604082019
050919050565b60006108a1603583610a48565b91506108ac82610ae4565b6040820190
50919050565b60006108c4602683610a48565b91506108cf82610b33565b60408201905
0919050565b60006108e7602d83610a48565b91506108f282610b82565b604082019050
919050565b600061090a602f83610a48565b915061091582610bd1565b6040820190509
19050565b600061092d603083610a48565b915061093882610c20565b60408201905091
9050565b61094c81610a8b565b82525050565b60006020820190506109760008301846
10862565b92915050565b60006020820190508181036000830152610986816108715 65
b9050919050565b60006020820190508181036000830152610 9a681610894565b90509
19050565b60006020820190508181036000830152610 9c6816108b7565b905091905056
5b60006020820190508181036000830152610 9e6816108da565b9050919050565b6000
60208201905081810360008301526 10a06816108fd565b9050919050565b60006020820
190508181036000830152610a2681610920565b9050919050565b600602082019050610
0a4260008301846109435 65b92915050565b60008282526020820190509291505056 5b
6000610a6482610a6b565b9050919050565b600073ffffffffffffffffffffffffffffffffffffffff8216
9050919050565b600081905091905056 5b7f54686520616d6f756e7420746f2072657475
726e206d75737420626520677265600082015 27f6174657220746861 6e207a65726f210
0000000000000000000000000000000000602082015250565b7f596f752063616e206e6f7
4206265207468652068696768657374426964646572600082015 27f20696e206f726465
7220746f2070726f6365656421000000000000000000000060208201525056 5b7f546865
726520697320616c726561647920612073616d65206f722068696768656000820152 7f7
220626964210000000000000000000000000000000000000000000000000000000060208201
5250565b7f596f752063616e206e6f74206265207468652 06f776e657220696e206f72646
560008201527f7220746f2070726f6365656421000000000000000000000000000000000000
0000060208201525056 5b7f596f752068616420616e20756e737563657373 66756c20
63616c6c206f662060008201527f6269742c207472792061676 1696e2100000000000000
0000000000000000000060208201525056 5b7f596f752068616420616e20756e7375636
365737366756c2063616c6c206f662060008201527f73656e642c2074727920616761696
e2100000000000000000000000000000000060208201525056 5b610c7881610a59565b81
14610c8357600080fd5b5056fea2646970667358221220a6800788f15b76834dc8a30ddf
320bbaac0d28e660e2fafb54c06b31a216dbdd64736f6c63430008030033'

>var auctionDeployed = abi.new({from:eth.accounts[0], data:bytecode, gas:2000000})

Ελέγξτε το υπόλοιπο του λογαριασμού 1 (ιδιοκτήτης) και του λογαριασμού 2 (πλειοδότης 1), το ποσό της υψηλότερης προσφοράς και τη διεύθυνση του υψηλότερου πλειοδότη.

> eth.getBalance(eth.accounts[0])

119998055642010000000

> eth.getBalance(eth.accounts[1])

26999906414000000000

> auctionInstance.highestBid.call()

0

> auctionInstance.highestBidder.call()

"0x119998055642010000000"

Στείλτε transaction για να εκτελέσετε τη λειτουργία bid() για να υποβάλετε προσφορά 5ETH από τον λογαριασμό 2 (Πλειοδότης 1).

> auctionInstance.bid({from:eth.accounts[1], value:5000000000000000000})

"0x50655f889fd558a78e7014613602ef78f5ea6f56085fd4182834fd9b8c28a01e"

Ελέγξτε το υπόλοιπο του λογαριασμού του smart contract, του λογαριασμού 2 και του λογαριασμού 3, το ποσό της υψηλότερης προσφοράς και τη διεύθυνση του υψηλότερου πλειοδότη.

>eth.getBalance("0x1ced06b870751fd8f36c332a6070792338a53e9e")

5000000000000000000

> eth.getBalance(eth.accounts[1])

21999906412000000000

> eth.getBalance(eth.accounts[2])

30002037944000000000

> auctionInstance.highestBid.call()

5000000000000000000

> auctionInstance.highestBidder.call()

"0xdff4738304f0461fe27d4a2cfe81c24939123775"

Στείλτε transaction για να εκτελέσετε την bid() για να υποβάλετε προσφορά 10ETH από τον λογαριασμό 3 (Πλειοδότης 2).

> auctionInstance.bid({from:eth.accounts[2], value:10000000000000000000})

"0xbd51398253dafb28c0f4fa052162fd3e07ffc98027662a54ecb51f73ca424bb7"

Ελέγξτε το υπόλοιπο του λογαριασμού του smart contract και του λογαριασμού 3, το ποσό της υψηλότερης προσφοράς και διεύθυνση του υψηλότερου πλειοδότη.

>eth.getBalance("0x1ced06b870751fd8f36c332a6070792338a53e9e")

1500000000000000000

> eth.getBalance(eth.accounts[2])

10001880772000000000

> auctionInstance.highestBid.call()

1000000000000000000

> auctionInstance.highestBidder.call()

"0xf401c6ecd8abd757303e9db46c293471c90faf75"

Στείλτε transaction για να εκτελέσετε τη λειτουργία withdraw() για να αποσύρετε το ποσό της προσφοράς του λογαριασμού 2.

>auctionInstance.withdraw({from:eth.accounts[1]})

"0x08a7d247df35bd2d41dd4b6d8d6adb7c2b3a41ff6c8289197bc6926808cfa35a"

Ελέγξτε το υπόλοιπο του λογαριασμού του smart contract και του λογαριασμού 2.

>eth.getBalance("0x1ced06b870751fd8f36c332a6070792338a53e9e")

1000000000000000000

> eth.getBalance(eth.accounts[1])

26999906414000000000