UNIVERSITY OF THESSALY
SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL
& COMPUTER ENGINEERING

Project: Develop and Deploy a Smart Contract on a Public Test Network

Μάθημα: Τεχνολογίες blockchain και αποκεντρωμένες εφαρμογές

Διδάσκων: ΦΩΤΗ ΜΑΓΔΑΛΗΝΗ

Ακ. έτος 2020-21, εαρινό εξάμηνο

Ονοματεπώνυμο: Καραμούστου Βασιλική

ΑΕΜ: 02424

Contents

Deployment σε public test network.

./geth --rinkeby --syncmode "light"

./geth attach /home/vasia/.ethereum/rinkeby/geth.ipc

Προετοιμάστε τρεις λογαριασμούς για τον έλεγχο του smart contact.

> personal.newAccount()

"0x515f2d8b24470da15fe5b7082f700cbe327de11d"

> personal.newAccount()

"0xe949c764b497e1d5295cbcd0104344ed14c2d0f0"

> personal.newAccount()

"0x8c3c20791ae6f242dfd14b4b143ed7645ab32298"

//unlock accounts

> web3.personal.unlockAccount(eth.accounts[0],"1234",6000)

true

> web3.personal.unlockAccount(eth.accounts[1],"1234",6000)

true

> web3.personal.unlockAccount(eth.accounts[2],"1234",6000)

true

//Fill all 3 accounts with enough eth

> eth.sendTransaction({from:eth.accounts[2],to:eth.accounts[0],value:1000000000000000000})

"0x317a5baf5331f1cbda7228e4ee2b338dfd260af8afc82086f573c001e4fad53c"

> eth.sendTransaction({from:eth.accounts[2],to:eth.accounts[1],value:6000000000000000000})

"0xc8b6784e84767e4258a6dffd3689078f6906f03361f15b020d8a5f430133f344"

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

======= Auction.sol:Auction =======

Contract JSON ABI

[{"inputs":[],"stateMutability":"nonpayable","type":"constructor"},{"inputs":[],"name":"bid","outputs":[],"stateMutability":"payable","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":"nonpayable","type":"function"}]

> solc --bin auction.sol

======= Auction.sol:Auction =======

Binary:

6080604052600060045534801561001557600080fd5b50336000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550600060038190555060006002819055506000805490610100a900473ffffffffffffffffffffffffffffffffffffffff1660016000610100a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160217905550610cbc806100d66000396000f3fe608060405260043610610055576000356e01c80631998aeef1461005a57806326224c64146100

645780633ccfd60b146100a15780636f9fb98a146100b857806391f90157146100e35780
63d57bde791461010e575b600080fd5b610062610139565b005b3480156100705760008
0fd5b5061008b60048036038101906100869190610839565b6104bc565b604051610098
9190610a2d565b60405180910390f35b3480156100ad57600080fd5b506100b66104d45
65b005b3480156100c457600080fd5b506100cd6107f0565b6040516100da9190610a2d5
65b60405180910390f35b3480156100ef57600080fd5b506100f86107f8565b6040516101
059190610952565b60405180910390f35b34801561011a57600080fd5b5061012361081
e565b604051610130919061a2d565b60405180910390f35b6000805490610100a90047
3ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffff
ffffffffffffffffffff1614156101c8576040517f08c379a0000000000000000000000000000000
0000000000000000000000000000000815260040161016bf906109cd565b60405180910390fd
5b60025434116102c576040517f08c379a0000000000000000000000000000000000000000
0000000000000000000000815260040161020390610ad565b60405180910390fd5b600
254600581905550600160009054906101000a900473ffffffffffffffffffffffffffffffffffffffff166
00660006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffff
ffffffffffffffffff160217905550346002819055503360016000610100a81548173ffffffffff
ffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055506007
60003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff1681526020
019081526020016000205434111561047657600060076003373ffffffffffffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020541461047
5573373ffffffffffffffffffffffffffffffffffffffff166108fc600760003373ffffffffffffffffffffffffffffffff
ffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020549081
150290604051600060405180830381858888f193505050506104745760055460028190
55506006600090549061010000a900473ffffffffffffffffffffffffffffffffffffffff166001600061010
00a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff
f160217905550600161047357604051 7f08c379a0000000000000000000000000000000
0000000000000000000000000000000815260040161046a906109ed565b60405180910390fd5
b5b5b5b34600760003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff
ffff168152602001908152602001600020819055055 65b60076020528060005260406000
20600091509050548 1565b60016000905490610100a900473ffffffffffffffffffffffffffffffffffffffff
ffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff161415610
565576040517f08c379a0000000000000000000000000000000000000000000000000000000
0000008152600401610 55c9061098d565b60405180910390fd5b6000600760003373fffff
fffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602
0016000205411806105fe575060008054906101000a900473ffffffffffffffffffffffffffffffffffffffff
fff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff16145b61063
d576040517f08c379a0000000000000000000000000000000000000000000000000000000
0000815260040161063490610 96d565b60405180910390fd5b6000805490610100a900
473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffff
ffffffffffffffffffff16141561069f576002546004819055506 1072b565b600760003373ffff
ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602

0016000205460048190555060006007600033737fffffffffffffffffffffffffffffffff1673ffffff
ffffffffffffffffffffffffffffffff16815260200190815260200160002081905550600161076ed576
040517f08c379a0000000000000000000000000000000000000000000000000000000000000000
81526004016107e490610a0d565b60405180910390fd5b5b565b60004790509056 5b600
160009054906101000a900473ffffffffffffffffffffffffffffffffffffffff1681565b60025481565b6
000813590506108338161 0c6f565b92915050565b60006020828403121561084b576000
80fd5b60006108598482850161 0824565b91505092915050565b61086b81610a59565b8
2525050565b600061087e602f83610a48565b91506108898261 0a95565b604082019050
919050565b60006108a1603583610a48565b91506108ac82610ae4565b6040820190509
19050565b60006108c4602683610a48565b91506108cf82610b33565b60408201905091
9050565b60006108e7602d83610a48565b91506108f282610b82565b604082019050919
050565b600061090a602f83610a48565b91506109158261 0bd1565b6040820190509190
50565b600061092d603083610a48565b91506109388261 0c20565b60408201905091905
0565b61094c81610a8b565b82525050565b60006020820190506109760008301846108
62565b92915050565b60006020820190508181036000830152610986816108715565b90
50919050565b60006020820190508181036000830152610 9a681610894565b90509190
50565b60006020820190508181036000830152610 9c6816108b7565b9050919050565b6
000602082019050818103600083015261 09e6816108da565b90509190 50565b60006020
820190508181036000830152610a06816108fd565b9050919050565b600060208201905
081810360008301526 10a26816109205 65b9050919050565b60006020 8201905
0818103600083015261 0a4260008301846109435 65b92915050565b60008282526020820190509291505056 5b600
0610a6482610a6b565b9050919050565b600073ffffffffffffffffffffffffffffffffffffffff8216905
0919050565b60008190509190505 65b7f54686520616d6f756e7420746f2072657475726
e206d7573742062652067726560008201527f6174657220746861 6e207a65726f210000
0000000000000000000000000000000060208201525 0565b7f596f752063616e206e6f7420
626520746865206869676865737442696464657260008201527f20696e206f726465722
0746f2070726f6365656421000000000000000000000060208201525 0565b7f546865726
520697320616c726561647920612073616d65206f722068696768656 0008201527f7220
626964210000000000000000000000000000000000000000000000000000000060208201525
0565b7f596f752063616e206e6f74206265207468652 06f776e657220696e206f72646560
008201527f7220746f2070726f6365656421000000000000000000000000000000000000
006020820152505 65b7f596f752068616420616e20756e737563657373667 56c206361
6c6c206f662060008201527f6269742c207472792061676 1696e2100000000000000000000
0000000000000000060208201525 0565b7f596f752068616420616e20756e73756363657
37366756c2063616c6c206f662060008201527f73656e642c207472792061676 1696e210
0000000000000000000000000000000060208201525 0565b610c7881610a59565b811461
0c8357600080fd5b5056fea2646970667358221220 56b98fa233688497d2bc206d0f65aa
238d2c43820d92f4481a2abd9c4f74bde764736f6c63430008030033

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

> var abi=eth.contract([{"inputs":[],"stateMutability":"nonpayable","type":"constructor"},{"inputs":[],"name":"bid","outputs":[],"stateMutability":"payable","type":"function","payable":true},{"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":"nonpayable","type":"function"}])

undefined

> var bytecode='0x60806040526000600455348015610015576000 80fd5b5033600080610100
0a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff
16021790555060006003819055506000600281905550600080549061010 00a900473fffff
ffffffffffffffffffffffffffffffff16600160006101000a81548173ffffffffffffffffffffffffffffffffffffffff
f021916908373ffffffffffffffffffffffffffffffffffffffff160217905550610cbc806100d660003960
00f3fe608060405260043610610055576000 3560e01c80631998aeef1461005a57806326
224c64146100645780633ccfd60b146100a15780636f9fb98a146100b857806391f901571
46100e3578063d57bde791461010e575b600080fd5b610062610139565b005b34801561
007057600080fd5b5061008b600480360381019061008691906108 39565b6104bc565b6
040516100989190610a2d565b60405180910390f35b3480156100ad57600080fd5b5061
00b66104d4565b005b3480156100c457600080fd5b506100cd6107f0565b6040516100d
a9190610a2d565b60405180910390f35b3480156100ef57600080fd5b506100f86107f85
65b604051610105919061095 2565b60405180910390f35b34801561011a57600080fd5b
5061012361081e565b604051610130919061 0a2d565b60405180910390f35b600805549
06101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163
373ffffffffffffffffffffffffffffffffffffffff1614156101c8576040517f08c379a000000000000000
0000000000000000000000000000000000000000000000008152600401610 1bf906109cd565b6
0405180910390fd5b600254341161020c576040517f08c379a0000000000000000000
0000000000000000000000000000000000000000000008152600401610203906109ad565b60405180
910390fd5b60025460058190555060016000905490610100 0a900473ffffffffffffffffffffffffffffffffffffffff
ffffffffffffff16600660006101000a81548173ffffffffffffffffffffffffffffffffffffffff02191690837
3ffffffffffffffffffffffffffffffffffffffff160217905550346002819055503360016000 6101000a8

1548173ffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffff160
217905550600760003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffff
ffff16815260200190815260200160002054341115610476576000600760003373ffffffffff
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001
60002054146104755733 73ffffffffffffffffffffffffffffffffffffffff166108fc600760003373ffffffff
ffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001
60002054908115029060405160006040518083038185888f193505050506104745760 0
554600281905550600660009054906101000a900473ffffffffffffffffffffffffffffffffffffffff166
00160006101000a81548173ffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffff
ffffffffffffffffffff160217905550600161047357604051 7f08c379a0000000000000000000
0000000000000000000000000000000000000815260040161046a906109ed565b604051
80910390fd5b5b5b5b5b34600760003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffff
ffffffffffffffffffff168152602001908152602001600020819055056 5b600760205280600
052604060002060009150905054815 65b60016000905490610100 0a900473ffffffffffffffff
ffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffff
fff161415610565576040517f08c379a0000000000000000000000000000000000000000
0000000000000000081526004016105 5c9061098d565b60405180910390fd5b60006007
60003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff1681526020
019081526020016000205411806105fe575060008054906101000a900473ffffffffffffffffff
ffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff163373ffffffffffffffffffffffffffffffffffff
16145b61063d576040517f08c379a0000000000000000000000000000000000000000000
0000000000000081526004016106349061096d565b60405180910390fd5b6000805490
6101000a900473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff1633
73ffffffffffffffffffffffffffffffffffffff16141561069f576002546004819055506107 2b565b600
760003373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff168152602
001908152602001600020546004819055506000600760003373ffffffffffffffffffffffffffffffffffffffff
ffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020819055505
5b3373ffffffffffffffffffffffffffffffffffffffff166108fc60045490811502906040516000604051 8
0830381858888f193505050506107ee5760045460076000337 3ffffffffffffffffffffffffffffffffffffffff
ffffff1673ffffffffffffffffffffffffffffffffffffffff168152602001908152602001600020819055505 0
60016107ed576040517f08c379a0000000000000000000000000000000000000000000
0000000000008152600401610 7e490610a0d565b60405180910390fd5b5b565b600047
905090565b60016000905490610100 0a900473ffffffffffffffffffffffffffffffffffffffff1681565b
60025481565b60008135905061083381610c6f565b92915050565b60006020828403121
561084b57600080fd5b60006108598482850161082456 5b9150509291505056 5b61086b
81610a59565b82525050565b600061087e602f83610a48565b915061088982610a95565
b604082019050919050565b60006108a1603583610a48565b91506108ac82610ae4565b
604082019050919050565b60006108c4602683610a48565b91506108cf82610b33565b6
040820190509190505 65b60006108e7602d83610a48565b91506108f282610b82565b60
408201905091905056 5b600061090a602f83610a48565b915061091582610bd1565b604
082019050919050565b600061092d603083610a48565b915061093882610c20565b6040

8201905091905056 5b61094c81610a8b565b82525050565b60006020820190506109676
0008301846108625 65b92915050565b60006020820190508181036000830152610986 8
1610871565b9050919050565b60006020820190508181036000830152610 9a681610894
565b9050919050565b60006020820190508181036000830152610 9c6816108b7565b905
0919050565b60006020820190508181036000830152610 9e6816108da565b905091905
0565b60006020820190508181036000830152610a06816108fd565b9050919050565b60
0060208201905081810360008301526 10a2681610920565b9050919050565b600060208
2019050610a4260008301846109435 65b92915050565b60008282526020820190509291
5050565b6000610a6482610a6b565b9050919050565b600073ffffffffffffffffffffffffffffffffffffff
ffffff8216905091905056 5b60008190509190505 65b7f54686520616d6f756e7420746f20
72657475726e206d75737420626520677265600082015 27f6174657220746 8616e207a6
5726f2100000000000000000000000000000000000060208201525056 5b7f596f752063616
e206e6f74206265207468652068696768657374426964646572600082015 27f20696e20
6f7264657220746f2070726f6365656421000000000000000000000060208201525056 5b
7f54686572652069732061 6c726561647920612073616d65206f722068696768656000 8
201527f722062696421000000000000000000000000000000000000000000000000000000000000
602082015250565b7f596f752063616e206e6f742062652074686520 6f776e657220696e
206f72646560008201527f7220746f2070726f6365656421000000000000000000000000000
0000000000000060208201525056 5b7f596f752068616420616e20756e7375636365737
366756c2063616c6c206f662060008201527f6269742c207472792061676169 6e2100000
0000000000000000000000000000060208201525056 5b7f596f752068616420616e2075
6e737563365737366756c2063616c6c206f662060008201527f73656e642c207472792 0
616761696e2100000000000000000000000000000000060208201525056 5b610c7881610
a59565b8114610c8357600080fd5b5056fea2646970667358221220 56b98fa233688497d
2bc206d0f65aa238d2c43820d92f4481a2abd9c4f74bde764736f6c63430008030033'

undefined

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

Undefined

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])

999192421000000000

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

6000000000000000000

> var auctionInstance=abi.at(auctionDeployed.address)

undefined

> auctionInstance.highestBid.call()

0

> auctionInstance.highestBidder.call()

"0x515f2d8b24470da15fe5b7082f700cbe327de11d"

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})

"0x68c665c822cf6521a7c6136edb5d1bebde5e2651f948af1421684e9096d3e0bb"

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.

> auctionDeployed.address

"0x06333f82ddb97555d0685aee5a6a3e331289e54b"

> eth.getBalance("0x06333f82ddb97555d0685aee5a6a3e331289e54b")

5000000000000000000

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

999902322000000000

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

11749958000000000000

> auctionInstance.highestBid.call()

5000000000000000000

> auctionInstance.highestBidder.call()

"0xe949c764b497e1d5295cbcd0104344ed14c2d0f0"

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})

"0x02ff49c26b0523a42a213e26bbbee9d9bd95a72949bb9a33db2acade29abb239"

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

> eth.getBalance("0x06333f82ddb97555d0685aee5a6a3e331289e54b")

15000000000000000000

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

1749874622000000000

> auctionInstance.highestBid.call()

10000000000000000000

> auctionInstance.highestBidder.call()

"0x8c3c20791ae6f242dfd14b4b143ed7645ab32298"

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

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

"0xb1cb9f8b3c6686bc141f2c8d0fe8e415e976942f6de14553ee0c91de8fdac2e5"

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

> eth.getBalance("0x06333f82ddb97555d0685aee5a6a3e331289e54b")

10000000000000000000

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

5999857221000000000

Τα links από το αντίστοιχο etherscan προς τα transactions.

https://rinkeby.etherscan.io/address/0x515f2d8b24470da15fe5b7082f700cbe327de11d

https://rinkeby.etherscan.io/address/0xe949c764b497e1d5295cbcd0104344ed14c2d0f0

https://rinkeby.etherscan.io/address/0x8c3c20791ae6f242dfd14b4b143ed7645ab32298

> eth.accounts

["0x515f2d8b24470da15fe5b7082f700cbe327de11d",
"0xe949c764b497e1d5295cbcd0104344ed14c2d0f0",
"0x8c3c20791ae6f242dfd14b4b143ed7645ab32298"]