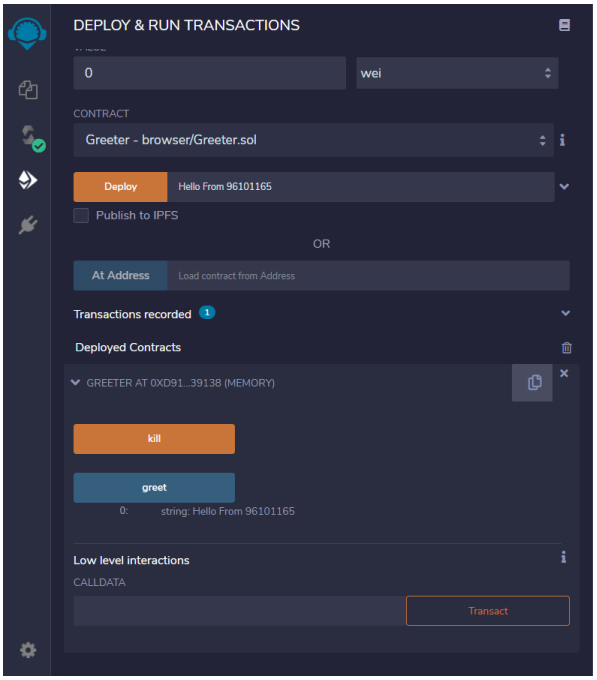
علی آراسته ۹۶۱۰۱۱۶۵

مبانی فناوری بلاکچین و رمزارزها – گزارش تمرین عملی سری سوم

سوال ۱:

موارد خواسته شده را به ترتیب انجام می‌دهیم. نتیجه به صورت زیر بدست می‌آید:




سوال ۲:

توابع خواسته شده را به صورت زیر پیاده‌سازی می‌کنیم:

ابتدا برای Contract مورد نظر تابع constructor را پیاده‌سازی می‌کنیم. این تابع یک متغیر از نوع uint256 دریافت می‌کند و مقدار _totalSupply و balance ارسال‌کننده پیام را برابر مقدار این متغیر قرار می‌دهد.

تابع totalSupply: این تابع مقدار _totalSupply را برمی‌گرداند.

تابع balanceOf: این تابع یک متغیر از نوع address دریافت می‌کند و مقدار balance این آدرس را برمی‌گرداند.

تابع transfer: این تابع یک متغیر از نوع address به عنوان آدرس گیرنده و یک متغیر از نوع uint256 به عنوان مقدار انتقالی دریافت می‌کند. در این تابع ابتدا بررسی می‌شود که حساب ارسال‌کننده پیام به اندازه کافی موجودی داشته باشد. اگر موجودی کافی باشد، به اندازه مقدار انتقالی از موجودی ارسال‌کننده پیام کم و به حساب گیرنده اضافه می‌شود. همچنین event مناسب یعنی Transfer با آرگومان‌های مناسب ثبت و مقدار true برای اعلام موفق بودن انتقال برگردانده می‌شود.

تابع allowance: این تابع دو متغیر از نوع address دریافت می‌کند، یکی آدرس صاحب حساب و دیگری آدرسی که می‌خواهد پولی را از این حساب به حساب دیگر منتقل کند، و مقداری را که آدرس دوم مجاز به برداشت از آدرس اول است، برمی‌گرداند.

تابع transferFrom: این تابع مانند تابع transfer است با این تفاوت که یک متغیر اضافه از نوع address دریافت می‌کند. در این تابع ابتدا بررسی می‌شود که آدرس اول به اندازه کافی موجودی داشته باشد و همچنین ارسال‌کننده پیام اجازه برداشت این مقدار را داشته باشد. اگر شرایط برقرار باشد، به اندازه مقدار انتقالی از موجودی آدرس اول کم و به حساب گیرنده اضافه می‌شود. همچنین مقدار برداشت مجاز از آدرس اول برای ارسال‌کننده پیام به طور مناسب به روز می‌شود و event مناسب یعنی Transfer با آرگومان‌های مناسب ثبت و مقدار true برای اعلام موفق بودن انتقال برگردانده می‌شود.

تابع approve: این تابع یک متغیر از نوع address به عنوان آدرس مجاز به برداشت و یک متغیر از نوع uint256 به عنوان مقدار مجار برداشت دریافت می‌کند و مقداری را که آدرس مورد نظر مجاز به برداشت از حساب ارسال‌کننده پیام است، تعیین می‌کند. همچین event مناسب یعنی Approval با آرگومان‌های مناسب ثبت و مقدار true برای اعلام موفق بودن عملیات برگردانده می‌شود.

سوال ۳:

توابع خواسته شده را به صورت مناسب پیاده‌سازی می‌کنیم. در ادامه درباره بعضی از این توابع توضیحاتی ارائه می‌شود:

اصلاح‌کننده canTransfer با استفاده از تابع isApprovedOrOwner، اجازه انتقال token مورد نظر توسط ارسال‌کننده پیام را بررسی می‌کند.

تابع transferFrom: این تابع در صورتی که شروط اصلاح‌کننده canTransfer ارضا شوند، در ابتدا با استفاده از تابع clearApproval، اجازه انتقال token مورد نظر را از افراد مجاز سلب می‌کند، سپس با استفاده از تابع removeTokenFrom، تعلق token مورد نظر به آدرس اول را پاک می‌کند و در آخر با استفاده از تابع addTokenTo، مالکیت token مورد نظر را به آدرس دوم می‌دهد.

تابع safeTransferFrom: مانند تابع tranferFrom است با این تفاوت که اگر آدرس دوم متعلق به یک Contract باشد، ابتدا بررسی می‌کند که Contract مورد نظر تابع onERC721Received را پیاده‌سازی کرده باشد.

سوال ۴:

توابع خواسته شده را به صورت مناسب پیاده‌سازی می‌کنیم. در ادامه درباره بعضی از این توابع توضیحاتی ارائه می‌شود:

ابتدا برای Contract مورد نظر تابع constructor را پیاده‌سازی می‌کنیم. این تابع در صورت بزرگتر از صفر بودن هر سه مقدار _commitment_len، _opening_len و msg.value، متغیرهای حالت Contract را به طور مناسب مقداردهی می‌کند.

اصلاح‌کننده‌های duringCommitment و duringOpening به ترتیب باعث می‌شوند، یک تابع تنها در فاز Commitment و Opening قابل فراخوانی باشد.

تابع activateAuction، مزایده را آغاز می‌کند و مقدار متغیر فاز را برابر Commitment قرار می‌دهد.

از زمان آغاز مزایده به اندازه _commitment_len بلاک، متقاضیان وقت دارند پیشنهادهای خود را با استفاده از تابع bid ارسال کنند.

تابع startOpening، سه متقاضی مجاز را مشخص می‌کند و مقدار متغیر فاز را برابر Opening قرار می‌دهد.

از زمان فراخوانی تابع startOpening به اندازه _opening_len بلاک، سه متقاضی مجاز فرصت دارند، value و nonce خود را با استفاده از تابع open اعلام کنند.

تابع finalize، مزایده را تمام می‌کند، بودجه درخواستی را برای برنده مزایده ارسال می‌کند و باقی‌مانده را به حساب شرکت برمی‌گرداند.

برای قسمت امتیازی تنها نیاز است آدرس فایل به صورت رمز شده ارسال شود.

سوال ۵:

موارد خواسته شده را به ترتیب انجام می‌دهیم. نتیجه به صورت زیر بدست می‌آید:

ایجاد Contract:

creation of CustomAuction pending...

https://ropsten.etherscan.io/tx/0xc5ab7081126df4ef57ee62ba5d20945bac374c2047365ed8a930b5597b005be1

[block:9284927 txIndex:48] from: 0x5fE...b8Cd5to: CustomAuction.(constructor)value: 10000000000000000 weidata: 0x608...00014logs: 0hash: 0xc5a...05be1

status true Transaction mined and execution succeed

transaction hash 0xc5ab7081126df4ef57ee62ba5d20945bac374c2047365ed8a930b5597b005be1

from 0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5

to CustomAuction.(constructor)

gas 1065331 gas

transaction cost 1065331 gas

hash 0xc5ab7081126df4ef57ee62ba5d20945bac374c2047365ed8a930b5597b005be1

input 0x608...00014

decoded input { "address _admin": "0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5", "uint256 _commitment_len": { "type": "BigNumber", "hex": "0x14" }, "uint256 _opening_len": { "type": "BigNumber", "hex": "0x14" } }

decoded output -

logs []

value 10000000000000000 wei

فراخوانی تابع activateAuction:

transact to CustomAuction.activateAuction pending ...

https://ropsten.etherscan.io/tx/0x8ac1337c2636c9cda544e9de19b56d0a49b15b13cbbd84d5f0aaf3ebdbebecca

[block:9284937 txIndex:13] from: 0x5fE...b8Cd5to: CustomAuction.activateAuction() 0xa5C...895A7value: 0 weidata: 0x605...fed87logs: 1hash: 0x8ac...becca

status true Transaction mined and execution succeed

transaction hash 0x8ac1337c2636c9cda544e9de19b56d0a49b15b13cbbd84d5f0aaf3ebdbebecca

from 0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5

to CustomAuction.activateAuction() 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 69691 gas

transaction cost 69691 gas

hash 0x8ac1337c2636c9cda544e9de19b56d0a49b15b13cbbd84d5f0aaf3ebdbebecca

input 0x605...fed87

decoded input {}

decoded output -

logs [ { "from": "0xa5C1d3d31638a002A6f29A7c8D42c437672895A7", "topic": "0xee2679bc2382e067cc3dfbda872852b5b1702b359c1fd6ce272c32dae5bacabf", "event": "auctionStarted", "args": {} } ]

value 0 wei

## ارسال پیشنهاد توسط متقاضیان:

transact to CustomAuction.bid pending ...

https://ropsten.etherscan.io/tx/0x0b301bc5636f0f4ef6f93c23aa726dfb6d6f18cb6b11e07ee14f6b91ce3e5bb8

[block:9284942 txIndex:54] from: 0x0f7...e703cto: CustomAuction.bid(bytes32,bytes32) 0xa5C...895A7value: 0 weidata: 0x434...46e6alogs: 0hash: 0x0b3...e5bb8

status true Transaction mined and execution succeed

transaction hash 0x0b301bc5636f0f4ef6f93c23aa726dfb6d6f18cb6b11e07ee14f6b91ce3e5bb8

from 0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c

to CustomAuction.bid(bytes32,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 67054 gas

transaction cost 67054 gas

hash 0x0b301bc5636f0f4ef6f93c23aa726dfb6d6f18cb6b11e07ee14f6b91ce3e5bb8

input 0x434...46e6a

decoded input { "bytes32 _bidHash": "0x56f0d5a4adcccеffe4ee2bdfe9816ddb6d2c05b151ca9840ceab2ab9f45aff80", "bytes32 _FileAddress": "0x8308096302d60da6bd1a583769fc46645f2d1b13390db148a1cb20bd75446e6a" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.bid pending ...

https://ropsten.etherscan.io/tx/0x9187e28771147b90bcf7dd680ccca5f97125cf5096625b7c322520e77a3f5eba

[block:9284945 txIndex:46] from: 0xCbC...acFbato: CustomAuction.bid(bytes32,bytes32) 0xa5C...895A7value: 0 weidata: 0x434...f1624logs: 0hash: 0x918...f5eba

status true Transaction mined and execution succeed

transaction hash 0x9187e28771147b90bcf7dd680ccca5f97125cf5096625b7c322520e77a3f5eba

from 0xCbC8d2CDe085cC7f6b105BED9A39B837671acFba

to CustomAuction.bid(bytes32,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 67054 gas

transaction cost 67054 gas

hash 0x9187e28771147b90bcf7dd680ccca5f97125cf5096625b7c322520e77a3f5eba

input 0x434...f1624

decoded input { "bytes32 _bidHash": "0x0329ebf14b410ee6d3b27b6b599c73b807695b6d1944fb8503f34f8b8b8dd3bc", "bytes32 _FileAddress": "0xb879c5e9a7219e36e4df6d068118b570933c447ff94698d03fe1fadd344f1624" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.bid pending ...

https://ropsten.etherscan.io/tx/0x30b06366809d566cc14c53724931d4c84959e8e438888587f977dc7122dcf1d2

[block:9284947 txIndex:7] from: 0x59c...55202to: CustomAuction.bid(bytes32,bytes32) 0xa5C...895A7value: 0 weidata: 0x434...c9ebalogs: 0hash: 0x30b...cf1d2

status true Transaction mined and execution succeed

transaction hash 0x30b06366809d566cc14c53724931d4c84959e8e438888587f977dc7122dcf1d2

from 0x59c5b2463531fA913681CF93A4EFa25365455202

to CustomAuction.bid(bytes32,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 67042 gas

transaction cost 67042 gas

hash 0x30b06366809d566cc14c53724931d4c84959e8e438888587f977dc7122dcf1d2

input 0x434...c9eba

decoded input { "bytes32 _bidHash": "0x1719ff2380695e51d4d5b307428c6df910e69b1e248ee137700e07e7d6f35e05", "bytes32 _FileAddress": "0x63fe380d9c188158e9e94f633f3f4e98bce6005df9c538af1606e02c757c9eba" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.bid pending ...

https://ropsten.etherscan.io/tx/0x6c0b876d9c4c46df215585313896f3f850f7f73ad821463f37211de2ac6c6d96

[block:9284949 txIndex:88] from: 0x866...1FbE4to: CustomAuction.bid(bytes32,bytes32) 0xa5C...895A7value: 0 weidata: 0x434...aa98blogs: 0hash: 0x6c0...c6d96

status true Transaction mined and execution succeed

transaction hash 0x6c0b876d9c4c46df215585313896f3f850f7f73ad821463f37211de2ac6c6d96

from 0x866d8F4cb24E8911E1eE9c7E81bb52c03Fa1FbE4

to CustomAuction.bid(bytes32,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 67042 gas

transaction cost 67042 gas

hash 0x6c0b876d9c4c46df215585313896f3f850f7f73ad821463f37211de2ac6c6d96

input 0x434...aa98b

decoded input { "bytes32 _bidHash": "0xfd279d0de0ee15a3614fb45191000b0364898282f33727e10165e93c14f8f6d2", "bytes32 _FileAddress": "0x7ec1ccbe782d4216df871e7a251572667d7dc22ef265b3bf35c34b8fd4faa98b" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.bid pending ...

https://ropsten.etherscan.io/tx/0x7ff581ef175b6ee90436164a4d54faf9b1957a6e23aad1e23ad52316730e6545

[block:9284951 txIndex:26] from: 0xB86...Ef358to: CustomAuction.bid(bytes32,bytes32) 0xa5C...895A7value: 0 weidata: 0x434...18c95logs: 0hash: 0x7ff...e6545

status true Transaction mined and execution succeed

transaction hash 0x7ff581ef175b6ee90436164a4d54faf9b1957a6e23aad1e23ad52316730e6545

from 0xB869c46C326b995893e28e7aF92b9A19682Ef358

to CustomAuction.bid(bytes32,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 67054 gas

transaction cost 67054 gas

hash 0x7ff581ef175b6ee90436164a4d54faf9b1957a6e23aad1e23ad52316730e6545

input 0x434...18c95

decoded input { "bytes32 _bidHash": "0x0a7673b2c840243f37fddbf65d8cbec7fd230c864246126d5e68452de15b50ed", "bytes32 _FileAddress": "0x95fd6affa0493251bad46af7ee8a700d1c4c8fc80775e4dcefb70eed0ec18c95" }

decoded output -

logs []

value 0 wei

## فراخوانی تابع startOpening:

transact to CustomAuction.startOpening pending ...

https://ropsten.etherscan.io/tx/0x52383af7451693803687d3a592e0a3101fe863eee8a58bd64e24a1341d7ec8bc

[block:9284960 txIndex:17] from: 0x5fE...b8Cd5to: CustomAuction.startOpening(address,address,address) 0xa5C...895A7value: 0 weidata: 0xeb5...55202logs: 1hash: 0x523...ec8bc

status true Transaction mined and execution succeed

transaction hash 0x52383af7451693803687d3a592e0a3101fe863eee8a58bd64e24a1341d7ec8bc

from 0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5

to CustomAuction.startOpening(address,address,address) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 100523 gas

transaction cost 100523 gas

hash 0x52383af7451693803687d3a592e0a3101fe863eee8a58bd64e24a1341d7ec8bc

input 0xeb5...55202

decoded input { "address add1": "0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c", "address add2": "0xCbC8d2CDe085cC7f6b105BED9A39B837671acFba", "address add3": "0x59c5b2463531fA913681CF93A4EFa25365455202" }

decoded output -

logs [ { "from": "0xa5C1d3d31638a002A6f29A7c8D42c437672895A7", "topic": "0xe884e87cca623860f1ac029c5df020e7b7ebad72eab657701673da4cf3e90461", "event": "openingStarted", "args": {} } ]

value 0 wei

## ارسال مقادیر value و nonce توسط متقاضیان مجاز:

transact to CustomAuction.open pending ...

https://ropsten.etherscan.io/tx/0x6e8de9736466fd336bb73d6fb1e5b4309a36243d90111f7729cefcc97d37c5fe

[block:9284962 txIndex:6] from: 0x0f7...e703cto: CustomAuction.open(uint256,bytes32) 0xa5C...895A7value: 0 weidata: 0x06c...0b29flogs: 0hash: 0x6e8...7c5fe

status true Transaction mined and execution succeed

transaction hash 0x6e8de9736466fd336bb73d6fb1e5b4309a36243d90111f7729cefcc97d37c5fe

from 0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c

to CustomAuction.open(uint256,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 116515 gas

transaction cost 101515 gas

hash 0x6e8de9736466fd336bb73d6fb1e5b4309a36243d90111f7729cefcc97d37c5fe

input 0x06c...0b29f

decoded input { "uint256 _value": { "type": "BigNumber", "hex": "0x174876e800" }, "bytes32 _nonce": "0xbbee2a3cddcae8e830a5d91ea677c1cc6605002763adc97e499c424dc470b29f" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.open pending ...

https://ropsten.etherscan.io/tx/0x9f50246ec21c0e64a9716e25137ebceb9e689e93e0142e349f4b081ac2eabb58

[block:9284967 txIndex:27] from: 0xCbC...acFbato: CustomAuction.open(uint256,bytes32) 0xa5C...895A7value: 0 weidata: 0x06c...0b29flogs: 0hash: 0x9f5...abb58

status true Transaction mined and execution succeed

transaction hash 0x9f50246ec21c0e64a9716e25137ebceb9e689e93e0142e349f4b081ac2eabb58

from 0xCbC8d2CDe085cC7f6b105BED9A39B837671acFba

to CustomAuction.open(uint256,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 70584 gas

transaction cost 70584 gas

hash 0x9f50246ec21c0e64a9716e25137ebceb9e689e93e0142e349f4b081ac2eabb58

input 0x06c...0b29f

decoded input { "uint256 _value": { "type": "BigNumber", "hex": "0x2e90edd000" }, "bytes32 _nonce": "0xbbee2a3cddcae8e830a5d91ea677c1cc6605002763adc97e499c424dc470b29f" }

decoded output -

logs []

value 0 wei

transact to CustomAuction.open pending ...

https://ropsten.etherscan.io/tx/0x92a5748c0ecaf9558ced8b442499ca9d5f950b9f1be2d08d6064929f60611145

[block:9284969 txIndex:30] from: 0x59c...55202to: CustomAuction.open(uint256,bytes32) 0xa5C...895A7value: 0 weidata: 0x06c...0b29flogs: 0hash: 0x92a...11145

status true Transaction mined and execution succeed

transaction hash 0x92a5748c0ecaf9558ced8b442499ca9d5f950b9f1be2d08d6064929f60611145

from 0x59c5b2463531fA913681CF93A4EFa25365455202

to CustomAuction.open(uint256,bytes32) 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 70584 gas

transaction cost 70584 gas

hash 0x92a5748c0ecaf9558ced8b442499ca9d5f950b9f1be2d08d6064929f60611145

input 0x06c...0b29f

decoded input { "uint256 _value": { "type": "BigNumber", "hex": "0x45d964b800" }, "bytes32 _nonce": "0xbbee2a3cddcae8e830a5d91ea677c1cc6605002763adc97e499c424dc470b29f" }

decoded output -

logs []

value 0 wei

## فراخوانی تابع finalize:

transact to CustomAuction.finalize pending ...

https://ropsten.etherscan.io/tx/0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

[block:9284984 txIndex:62] from: 0x5fE...b8Cd5to: CustomAuction.finalize() 0xa5C...895A7value: 0 weidata: 0x4bb...278f3logs: 1hash: 0x29f...a3da5

status true Transaction mined and execution succeed

transaction hash 0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

from 0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5

to CustomAuction.finalize() 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 90192 gas

transaction cost 90192 gas

hash 0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

input 0x4bb...278f3

decoded input {}

decoded output -

logs [ { "from": "0xa5C1d3d31638a002A6f29A7c8D42c437672895A7", "topic": "0xd0cf8e3f18ba7294910551daebfd3ec1e6dc1ce599a026f41196f54bc6aafbb4", "event": "auctionFinished", "args": { "0": "0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c", "1": "100000000000", "winnerAddress": "0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c", "winnerBid": "100000000000" } } ]

value 0 wei

سوال ۶:

موارد خواسته شده را به ترتیب انجام می‌دهیم. نتیجه به صورت زیر بدست می‌آید:

ایجاد Contract:

transact to CustomAuction.finalize pending ...

https://ropsten.etherscan.io/tx/0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

[block:9284984 txIndex:62] from: 0x5fE...b8Cd5to: CustomAuction.finalize() 0xa5C...895A7value: 0 weidata: 0x4bb...278f3logs: 1hash: 0x29f...a3da5

status true Transaction mined and execution succeed

transaction hash 0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

from 0x5fE7AF50ccB3aA80bBDce38ED2Ff7c13cadb8Cd5

to CustomAuction.finalize() 0xa5C1d3d31638a002A6f29A7c8D42c437672895A7

gas 90192 gas

transaction cost 90192 gas

hash 0x29fb8d928e9e6648992acd4b4cf433029a655e26be6717f83b20204e40ba3da5

input 0x4bb...278f3

decoded input {}

decoded output -

logs [ { "from": "0xa5C1d3d31638a002A6f29A7c8D42c437672895A7", "topic": "0xd0cf8e3f18ba7294910551daebfd3ec1e6dc1ce599a026f41196f54bc6aafbb4", "event": "auctionFinished", "args": { "0": "0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c", "1": "100000000000", "winnerAddress": "0x0f7c462f5C7fCC9Ae66A3F188D8F69085Afe703c", "winnerBid": "100000000000" } } ]

value 0 wei

# Results

| Candidate | Votes |
| --- | --- |
| 0 | 4 |
| 1 | 4 |
| 2 | 2 |
| 3 | 0 |

Candidate ID

Wallet Address

0x3b4cae73b9c60d345823e4b0a9b6ab4d11c5ffc0

Vote

Close