

Разработка смарт-контракта

Курсовая работа
студента 251 группы А. А. Григорьева

Саратовский государственный университет
им. Н. Г. Чернышевского

Кафедра математической кибернетики
и компьютерных наук

Научный руководитель: доцент Семенов М. С.

2018г.

- 1 Ознакомиться с особенностями разработки смарт-контрактов на **Ethereum** и языком программирования **Solidity**;
- 2 Рассмотреть процессы создания контрактов и взаимодействия с ними;

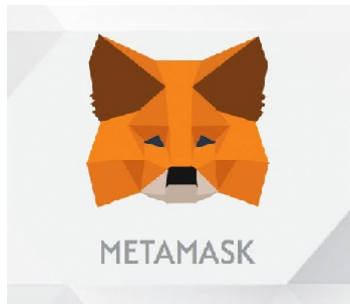
Ethereum — платформа для публикации смарт-контрактов.

Для умных контрактов характерно следующее:

- ❶ код функций выполняется на децентрализованной **Ethereum Virtual Machine**;
- ❷ прозрачность;
- ❸ результат их работы детерминирован;
- ❹ после добавления в блокчейн исходный код изменить невозможно.

Solidity — Javascript-подобный язык программирования умных контрактов. В курсовой работе использовались следующие возможности языка:


- 1 наследование контрактов;
- 2 модификаторы: пользовательские, видимости, предназначения функций;
- 3 особые типы данных: адреса и отображения;
- 4 работа с криптовалютой ether.



Remix IDE — многофункциональная среда разработки смарт-контрактов.

Metamask предоставляет интерфейс для совершения транзакций и управления кошельком.

Интерфейс умного контракта:

SimpleContract at 0x230...6301c (blockchain) 

contribute

kill

setNumber

contractInfo

contractOwner

donatorValues

getContributionTokenAmount

getDepartment

getNumber

weiDeposited

contribute - transact (payable)

uint256 newNumber

address

address user

Выполнение транзакций с помощью Metamask

SimpleContract

Deploy

Load contract from

1

MetaMask Notification

CONFIRM TRANSACTION

Ropsten Test Net

Main account
87F249..B00c
2.997 ETH
2129.13 USD

New Contract

Amount
0.00 ETH
0.00 USD

Gas Limit
722826 UNITS

Gas Price
7 GWEI

Max Transaction Fee
0.005059 ETH
3.59 USD

Max Total
0.005059 ETH
3.59 USD

Data included: 2449 bytes

RESET SUBMIT REJECT

Value 20 gwei

MetaMask Notification

CONFIRM TRANSACTION

Ropsten Test Net

Main account
87F249..B00c
2.991 ETH
2125.78 USD

230c43..301c

Amount
0.00 ETH
0.00 USD

Gas Limit
73056 UNITS

Gas Price
20 GWEI


Max Transaction Fee
0.001461 ETH
1.04 USD

Max Total
0.001461 ETH
1.04 USD

Data included: 4 bytes

RESET SUBMIT REJECT

Первый пользователь внес 20 gwei в контракт.

▼ SimpleContract at 0x230...6301c (blockchain) 

contribute

kill

setNumber

contractInfo

contractOwner

donatorValues

0: uint256: 20000000000

getContributionTokenAmount

0: uint256: 9999

getDepartment

getNumber

weiDeposited

0: uint256: 20000000001

Второй пользователь внес 180 gwei в контракт.

SimpleContract at 0x230...6301c (blockchain)

contribute

kill

setNumber

uint256 newNumber

contractInfo

0: address: 0x87F24960F6BA9Ed2b3d2e3Ac87714C0e9F3fB00c
1: string: SSU: Computer Science & Information Technologies

contractOwner

0: address: 0x87F24960F6BA9Ed2b3d2e3Ac87714C0e9F3fB00c

donatorValues

0xab27052f770f2e1cd0ebeaa0c1cf590f84e33260

0: uint256: 180000000180

getContributionTokenAmount

0xab27052f770f2e1cd0ebeaa0c1cf590f84e33260

0: uint256: 9000

getDepartment

getNumber

weiDeposited

0: uint256: 200000000181

В результате курсовой работы:

- 1 изучены основные возможности языка программирования контрактов **Solidity**;
- 2 рассмотрены условия работы с умными контрактами;
- 3 был развернут автономный контракт, доступ к которому можно получить в любое время.

- 1 Программный код контракта можно модифицировать для выполнения реальной задачи;
- 2 Имеется возможность связать смарт-контракт с внешней инфраструктурой посредством создания сайта или приложения.

СПАСИБО ЗА ВНИМАНИЕ!