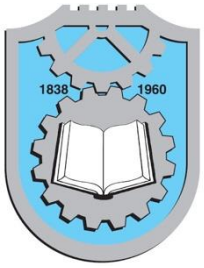
Универзитет у Крагујевцу
ФАКУЛТЕТ ИНЖЕЊЕРСКИХ НАУКА



Програмски преводиоци

Семинарски рад

Solidity

Паметни уговори

Професор:
Владимир Миловановић

Студент:
Матеја Вујсић 617/2017

Крагујевац **, 2021. године**

САДРЖАЈ

УВОД

Блокчејн (енг. Blockchain) технологија почела је са развојем биткоина(енг. Bitcoin) и проширила се на до сада познатих 2.000 криптовалута(енг. Cryptocurrencies) и данас учествују у тржишту са неколико милијарди долара. Многе криптовалуте се и даље развијају, многе су промашаји, док неке и даље траже финансије са стране за развој њихове дигиталне валуте. Доступност у креирању нових криптовалута за мала улагања, привукла је много људи. Поред тога предности блокчејна, његова поузданост, додатно стимулишу развој криптовалута и сматра се да ће дигиталне валуте у скоријој будућности заменити наш појам о новцу.

Питање је времена када ће криптовалуте ући у свакодневни живот. Многи визионари овог времена су сагласни да су дигиталне валуте будућност новца. О томе сведочи и ова изјава:

> *"The future of money is digital currency."*
>
> —Bill Gates

У овом семинарском раду биће речи о паметним уговорима (енг. Smart contracts) и програмском језику Солидити.

1. Паметни уговори(енг. SMART CONTRACTS)

Паметни уговори су компјутерски програми који су део у блокчејну и који се покрећу када се унапред одређени услови испуне.Најчешће се користе да аутоматизују неке радње , које се када се одређени услови испуне, потписници уговора добијају шта им следује без посредника и без губљења времена. Такође могу бити саставни део неког тока, покретајући неку акцију након се одређени услови испуне.

Како паметни уговори раде? Паметни уговори раде на принциу једноставног „if/when..then…" који су уграђени у блокчејн. Умрежени компјутери извршавају овај програм када се предодређени услови испуне и верификују.

Слика 2. *Традиционално склапање уговора између две стране*

Слика3. *Приступ склапању паметних уговора*

1.1 Бенефити паметних уговора

- **Аутономија** – Паметни уговорима не треба посредник да потврди уговор. Имплементација паметних уговора је таква да смањује ризик од манипулације треће стране која је у традиционалном склапању уговора кључна.
- **Опоравак –** Сви подаци који се налазе у блокчејну ускладиштени су неколико пута. Због те чињенице подаци се могу повратити и у случају губитка одређених података - квара.
- **Сигурност –** Паметни уговори су шифровани, и криптографија је та која се брине за сигурност и аутентичност података.
- **Брзина –** Темеље се на аутоматизованим компјутерским протоколима, што штеди време. Самим тим се и заобилази традиционална бирократија.
- **Тачност –** Коришћење паметних уговора заобилази грешке које произилазе из попуњавања физичких формулара.

1.2 Недостаци паметних уговора

- **Неподложност промени –** Готово је немогуће изменити испоручен паметан уговор. Њихова промена је процес који одузима много времена, свака грешка у коду је катастрофална и скупа.
- **Појава “loopholes” – вакума –** Некад је немогуће усагласити договорене услове уговора који закључују уговор са реалним исуњењем услова.
- **Неочекивани догађаји –** немогуће је у услове паметног уговора укључити услове које су неизвесни и њихово тумачење оствареног је дискутабилно.

2. SOLIDITY

Solidity је објектно-оријентисани програмски језик за писање паметних уговора. Синтаксно је сличан са *javascript-ом*, c++, python-ом. Користи се за имплементацију паметних уговора на различитим блокчејн платформама. Развијен је од стране *Christian Reitwiessner, Alex Beregszaszi* и још неколико програмера који су радили на развијању etherium core-а и написан је за имплементацију паметих уговора у блокчејн платформи Етеријум. Компајлирани *solidity* код намењен је да ради на Етеријум виртуално машини(EVM).

Представљен је 2014. године од стране Гавина Вуда. На развоју овог програмског језика радила је мала група искусних програмера. Солидити је примаран језик Етеријум платформе а такође и у већини приватних блокчејн платформи који су изграђени на Етеријуму као што су *HyperLedger Burrow Blockchain и Monax.*

Синтаксно, Солидити је дизајниран по ECMAscript правилима како би се што више приближи веб девелоперима. Највише фамилијарности има са програмски језицима пајтон, c++, javascript. Објектно-оријентисани програмски језик Солидити подржава наслеђивање, такође и вишеструко наслеђивање.

2.2 Пример кода

```
pragma solidity >= 0.7.0 <0.8.0;

contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping (address => uint) public balances;

    // Events allow clients to react to specific
    // contract changes you declare
    event Sent (address from, address to, uint amount);

    // Constructor code is only run when the contract
    // is created
    constructor() public {
        minter = msg.sender;
    }

    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount < 1e60);
        balances[receiver] += amount;
    }

    // Sends an amount of existing coins
    // from any caller to an address
    function send(address receiver, uint amount) public {
        require(amount <= balances[msg.sender], "Insufficient balance.");
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent (msg.sender, receiver, amount);
    }
}
```

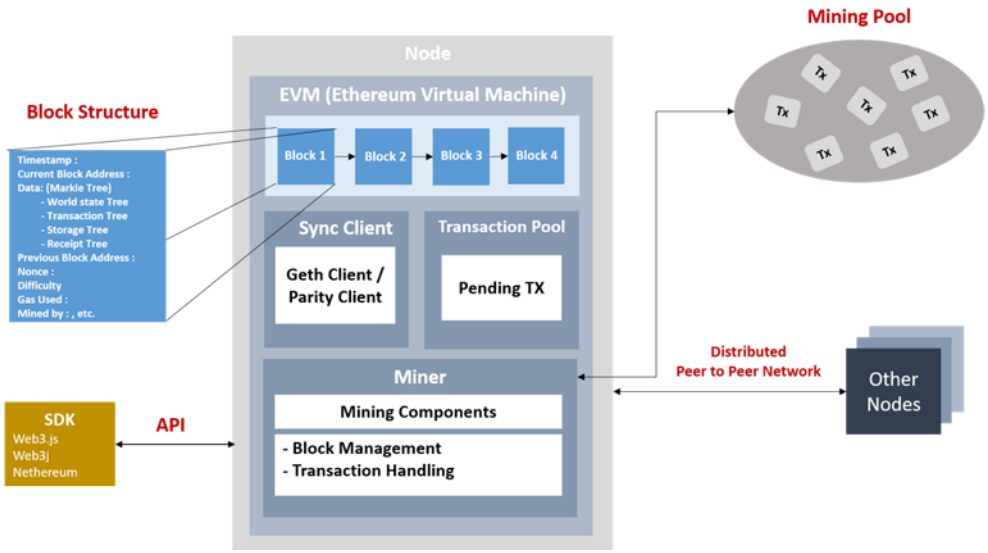
Сл4. Пример Солидити паметног уговора

Солидити је **Тјурин потпун језик**.

2.3 EVM – Etherium virtual machine

Etherium virtual machine(EVM) је веома моћан програм уграђен у сваки Етеријум чвор и одговоран је за извршавање паметних уговора. Уговори су написани најчешће у Солидитију а касније су компајлирани у EBM бајткод. Сваки чвор на Етеријум мрежи покреће једну EBM инстанцу, и циљ EBM је да компјутери на Етеријум мрежи покрену исту инструкцију. EBM је Тјурин потпун систем. То је заправо дистрибуирана state машина.

Када се уговор избаци на мрежу,тачније угради у блокчејн, сваки чвор на Етеријум мрежи добије бајткод тог уговора који се прослеђује EBM. Смарт уговори се покрећу трансакцијама, а трансакција мења стање блокчејна, што значи да се бајкод извршио.



Слика5. Етеријум мрежа

ЛИТЕРАТУРА

[1]https://corporatefinanceinstitute.com/resources/knowledge/deals/smart-contracts/, приступано 2.9.2021.

[2] **https://en.wikipedia.org/wiki/Solidity,** приступано 2.9.2021.

[3] https://www.ibm.com/topics/smart-contracts , приступано 3.9.2021.