УДК 628.336.42

АЛГОРИТМ ДОСТИЖЕНИЯ КОНСЕНСУСА ПОСРЕДСТВОМ БЛОКЧЕЙНА ETHEREUM

Жовнерик А.В., студентка группы 863102

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Саломатин С.Б. – к.т.н.,доцент

Аннотация. Актуальность данной работы связана с большим количеством взломов приложений, которые имеют централизованную структуру и непрозрачность в обработке и сбора данных посредниками. Цель работы - продемонстрировать феномен децентрализации через смарт-контракт Voting, развернутый в сеть Rinkeby.

Ключевые слова. Блокчейн Ethereum, смарт-контракт, криптография, распределенные системы.

Информационно-коммуникационные технологии (ИКТ) традиционно основываются на централизованной парадигме, в которой база данных или серверы приложений находятся под чьим-то единоличным управлением.

Децентрализация является основным преимуществом, предоставляемым технологией блокчейн, ее ключевым сервисом. Консенсус – основание блокчейна, которое обеспечивает децентрализацию и контроль при помощи майнинга.

В качестве платформы для построения приложения были проанализированы возможности Ethereum, TON и Hyperledger.

Ethereum – проект, в роли ключевой идеи которого выступает разработка тьюринг-полного языка, который позволяет создавать программное обеспечение произвольной сложности (smart contracts) для блокчейна и децентрализованных приложений [1]. Новшество Ethereum заключается в том, что любая выполняемая внутри него операция одновременно выполняется каждым отдельным узлом во всей сети. Состояние Ethereum включает в себя огромное количество транзакций. Эти транзакции группируются в «блоки».

Блок содержит группы транзакций, а каждый блок связан с предыдущим, тем самым образуя цепочку.

EVM (Ethereum Virtual Machine) – стековая, полностью изолированная среда выполнения, которая изменяет состояние системы с помощью инструкций в виде байт-кода [2]. Память не ограничена по размеру, но требует уплаты комиссии в виде газа. Хранилище виртуальной машины позволяет обращаться к данным по ключу и является частью состояния системы. Ключи и значения занимают по 32 байта. Программный код находится в виртуальной памяти, доступной только для чтения(анг. Virtual read-only memory, или VROM). VROM хранит код программы, который копируется в основную память. Затем EVM считывает основную память, ссылаясь на счетчик программы, и последовательно выполняет лексемы кода. Счетчик и стек виртуальной машины обновляются соответствующим образом после выполнения каждой инструкции(см. рисунок 1).

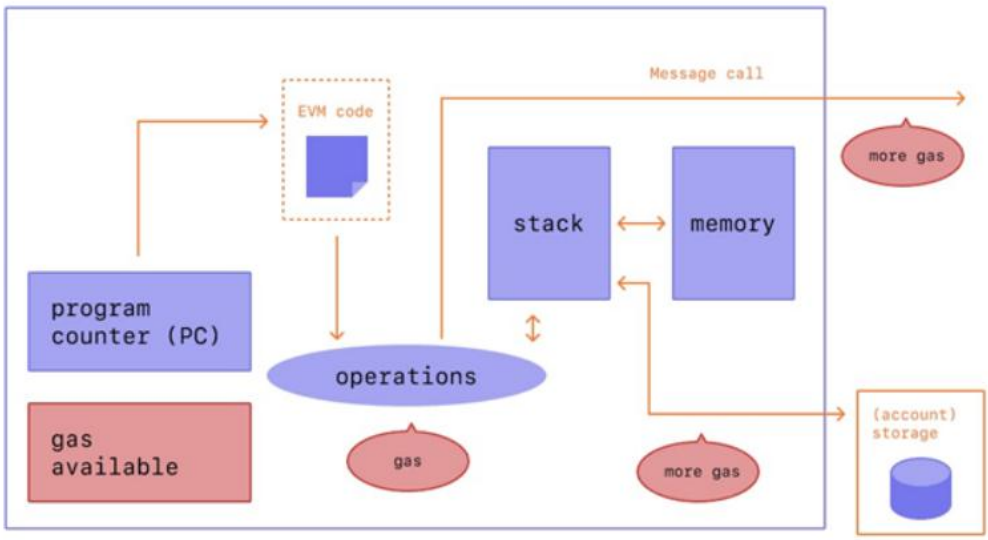

Рисунок 1 – Схема работы EVM

Учетная запись состоит из криптографической пары ключей: public и private. Public key генерируется из private key с помощью алгоритма ECDSA.

Смарт-контракт – это компьютерный алгоритм, который контролирует выполнение обязательств сторон в процессе обмена активами в технологии блокчейн [3]. Когда смарт-контракт работает на блокчейне, он автоматически запускается, когда выполняются все необходимые условия. Вся структура основана и проверена множеством подключенных компьютеров(см. рисунок 2) Это гарантирует, что смарт-контракты: безопасные, открытые, заслуживают доверия, почти лишены любых возможных ошибок.

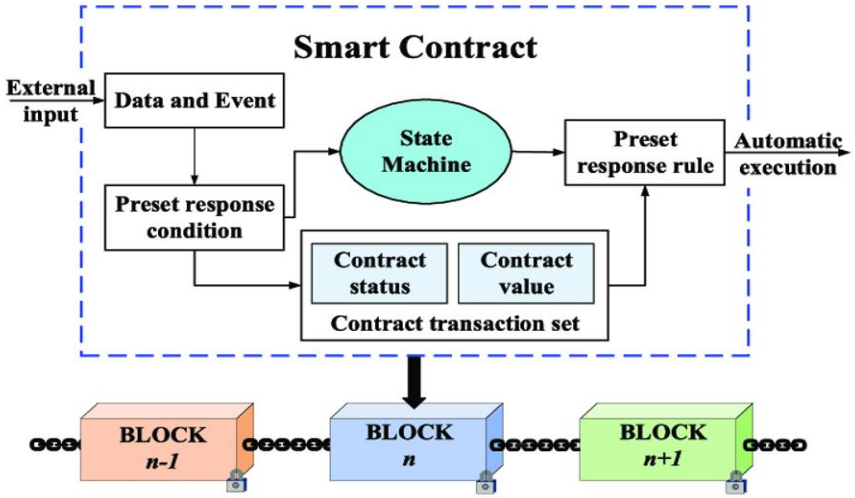

Рисунок 2 – Функционирование смарт-контракта в Ethereum

В рамках дипломной работы был разработан смарт-контракт(см. рисунок 3) на платформе Ethereum, предназначенный для голосований с возможностью других пользователей выбрать победителя и развернутый в тестовой сети Rinkeby.

Rinkeby — тестовая сеть Ethereum, которая позволяет проводить тестирование разработки блокчейна перед развертыванием в Mainnet, основной сети Ethereum [4].

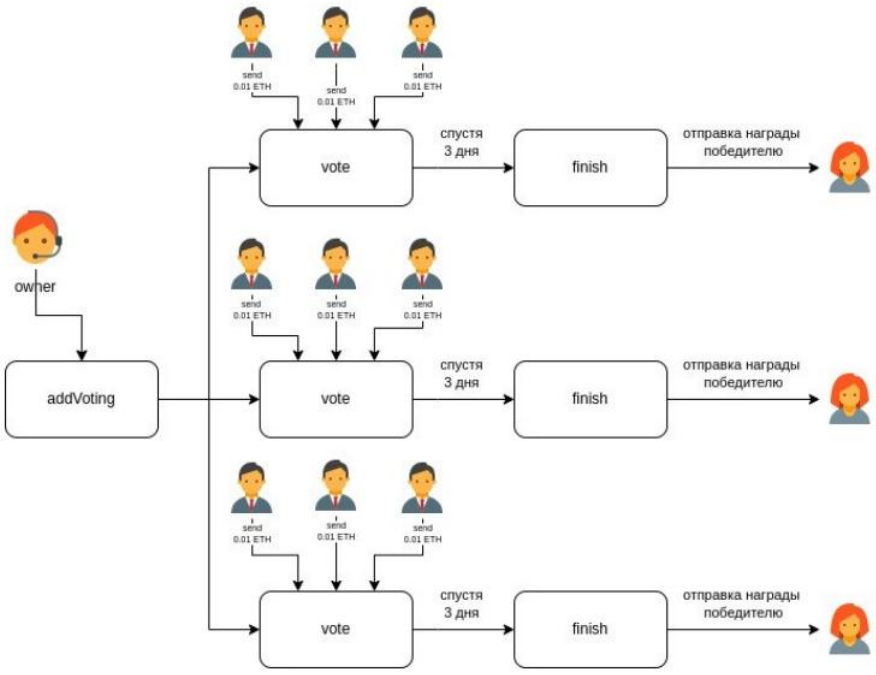

Рисунок 3 – Смарт-контракт Voting

Работа представляет интерес с практической точки зрения. Смарт-контракт, созданный в рамках данной дипломной работы, может быть использован для организации онлайн-голосования пользователей в сети Интернет.

Список использованных источников:

1. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты/пер. с анг.М.А. Райтмана. – М.:ДМК Пресс, 2019. – 538 с.: ил.
2. Yellow Paper Ethereum [Электронный ресурс]. – Режим доступа: Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain
3. Смарт-контракт, Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Смарт-контракт
4. Ethereum: работа с сетью, смарт-контракты и распределенные приложения / А. Бурков — «ЛитРес: Самиздат», 2020

UDC 628.336.42

Consensus algorithm through the ethereum blockchain

Zhauneryk A.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Salomatin S.B. – candidate of technical sciences

Annotation. The relevance of this work is due to the large number of hacks of applications that have a centralized structure and lack of transparency in the processing and collection of data by intermediaries. The goal is to demonstrate the phenomenon of decentralization through a smart contract voting based on the Ethereum blockchain, deployed in the Rinkeby network.

Keywords. Blockchain Ethereum, smart contract, cryptography, distributed systems.