В.П. Слепченко, Ю.Е. Карякин

Тюменский государственный университет, г. Тюмень

УДК 004.9

ТЕХНОЛОГИЯ СОЗДАНИЯ ДЕЦЕНТРАЛИЗОВАННОГО ПРИЛОЖЕНИЯ

Аннотация. В статье рассматривается проблема недоступности начинающим разработчикам попробовать себя в создании децентрализованного приложения из-за высокого порога вхождения. Это связано с тем, что нет полноценного и главного понятного источника, который осветил бы все аспекты работы, рассказал про инструментарий и вспомогательные приложения. Для решения обозначенной проблемы была написана данная статья, включающая в себя всю необходимую информацию для начала работы и создания собственного децентрализованного приложения на примере веб-приложения.

Ключевые слова: блокчейн, децентрализованное приложение, веб-приложение, инструментарий разработки, безопасность данных, криптографическое хранение.

В 2011 году была запущена пиринговая платёжная система Bitcoin на основе технологии блокчейн 1.0. Тогда данная технология находила своё использование исключительно в сфере криптовалют. В конце 2017 – начала 2018 года появилась технология блокчейн 3.0, получившая большую популярность из-за возможности создания DApp (Decentralized Application – Децентрализованное приложение).

DApp – приложение, разработанное на технологии блокчейн. По сравнению со стандартными приложениями у Dapp есть 2 основные особенности – устойчивость к DDoS атакам и открытый код.

Так как разработка ведется с помощью технологии блокчейн следует выделить ряд дополнительных преимуществ:

информация хранится в блоках, которые создаются с помощью криптографической проверки;

данные невозможно потерять или отменить только что созданные, также все предыдущие записи хранятся в неизменном виде и доступны любому участнику сети;

разрабатываемое приложение не будет иметь единого центра управления, по причине использования p2p-сети;

автономность работы нодов (Нода – любое устройство, подключенное к блокчейн-сети.), устройство не ставит задач перед другими узлами в сети и не получает никаких задач от них.

Встает вопрос: как определить, что приложение действительно является децентрализованным?

Для этого выделим критерии DApp которые однозначно дадут понять, что перед нами именно децентрализованное приложение.

Открытый код. Он необходим для достижения консенсуса среди участников сети;

Приложение не должно иметь центра управления и должно работать автономно;

Вся хранимая информация приложения должна криптографически храниться в публичном доступе;

В качестве доказательства работы нодов должен использоваться один из алгоритмов консенсуса (Proof-of-work, proof-of-stake и/или другие);

Приложение должно иметь свой токен (*токен* - единица учета, предназначенная для представления цифрового баланса в некотором активе, иными словами выполняющая функцию «заменителя денег» в цифровом мире, предназначены для привлечения инвестиций, необходимых для развития существующих проектов разработки.) для вознаграждения работы (за майнинг или инвестиции).

Рассмотрим инструментарий, необходимый для реализации децентрализованного приложения.

Для создания DApp была выбрана платформа Ethereum, поскольку она разработана специально для создания приложений на основе блокчейна и осуществляет поддержу смарт-контрактов (*смарт-контракт* – компьютерный алгоритм, предназначенный для поддержки работы и функционала контрактов в технологии блокчейн.).

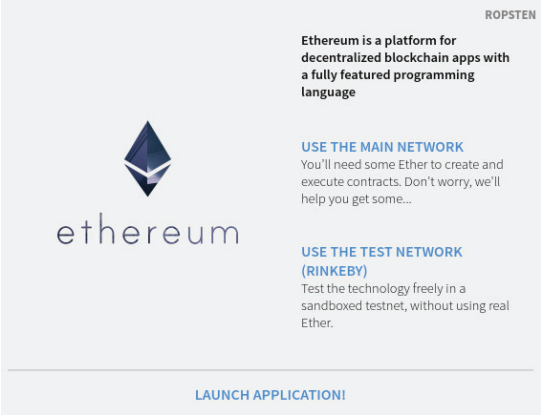

Рис. 1. Приложение Ethereum Wallet

Стоит отметить, что приложение будет работать в тестовой сети блокчейн. Это сделано в целях экономии времени, т.к. для запуска приложения в глобальной сети необходимо сначала скачать все существующие на данный момент блоки, что может занять продолжительное время. Тестовая сеть имитирует глобальную и разницы в способах разработки между ними нет.

Средой разработки для приложения решено было выбрать Truffle.

Truffle – среда разработки, представляющая собой тестовую инфраструктуру для Ethereum, целью которой является упростить работу со смарт-контрактами. Truffle поддерживает следующие функции:

встроенная интеллектуальная компиляция контрактов их связывание между собой и развертывание;

автоматизированное тестирование и проверка контракта на ошибки;

настраиваемый сборка контракта с поддержкой пользовательского интерфейса;

управление сетью для развертывания контракта во многих локальных и общедоступных сетях;

выполнение внешнего сценария.

После установки Truffle необходимо установить приложение Ganache CLI.

Ganache CLI является набором инструментов для разработки на Ethereum, он представляет собой модификацию для командной строки и добавляет ряд команд для разработки тестовой сети blockchain. На рисунке 2 представлено приложение Ganache CLI.

Ganache CLI предоставляет удобный интерфейс работы с тестовой сетью, здесь отображаются все аккаунты в сети, их private keys, количество эфира на каждом счету, существует функция создание токенов с определенным курсом, уникальный адрес для получения и отправки эфира или токенов, отслеживание выполнения транзакций между счетами и их логи.

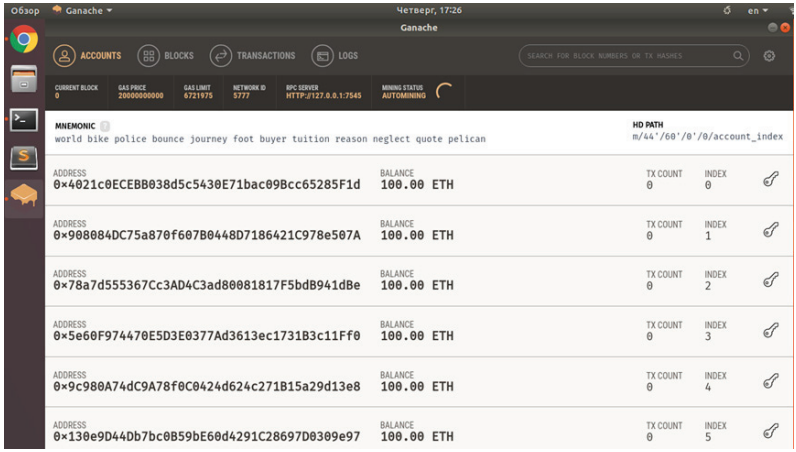

Рис. 2. Приложение Ganache CLI

После установки появляется возможность создать собственную тестовую сеть blockchain с несколькими аккаунтами, загружать в неё смарт-контракты и производить транзакции с помощью них. Для работы с тестовой сетью понадобится расширение MetaMask.

MetaMask – расширение для браузера, позволяющее посещать тестовую сеть от лица определенного аккаунта из Ganache CLI, производить транзакции, проверять их состояние и отслеживать состояние счета.

Для валидации форм на сайте и отправки данных в тестовую сеть блокчейн онадобится программная платформа Node.js. Для установки Node.js необходим NPM.

NPM представляет собой менеджер пакетов, входящих в состав Node.js. Данный менеджер понадобится для установки и загрузки внешних пакетов данных, запуска HTTP-сервера и добавит возможность вызывать внешние библиотеки из JavaScript кода, последняя функция понадобится для обработки информации об аккаунте пользователя и совершенных им транзакций.

Перейдем к структуре децентрализованного приложения. Децентрализованное приложение будет реализовать функционал голосования.

Структура DApp представляет собой открытую для просмотра базу данных, где все ячейки информации связаны друг с другом криптографически и имеют неизменяемую структуру.

На рисунке 3 показана структура децентрализованного приложения.

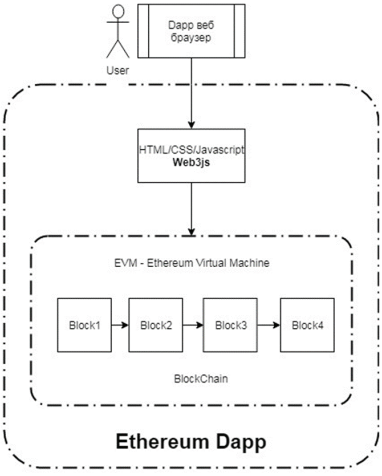

Рис. 3. Схема децентрализованного приложения

Рассмотрим поподробнее что происходит в блоке Blockchain и как вызывается непосредственно сам смарт-контракт.

В целом схема действий в блоке блокчейна представлена на рисунке 4.

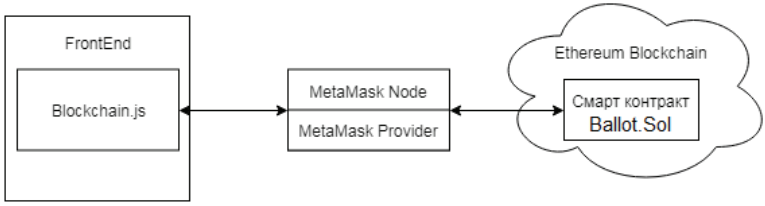

Рис. 4. Схема работы блока Blockchain

Модуль Blockchain.js отвечает за работу с блокчейном. Он работает с Web3.js и через ноду MetaMask напрямую обращается к блокчейну.

Рассмотрим архитектуру построения основного смарт-контракта Ballot.sol, реализующего работу с пользователем во время проведения голосования.

Схема смарт-контракта изображена на рисунке 5.

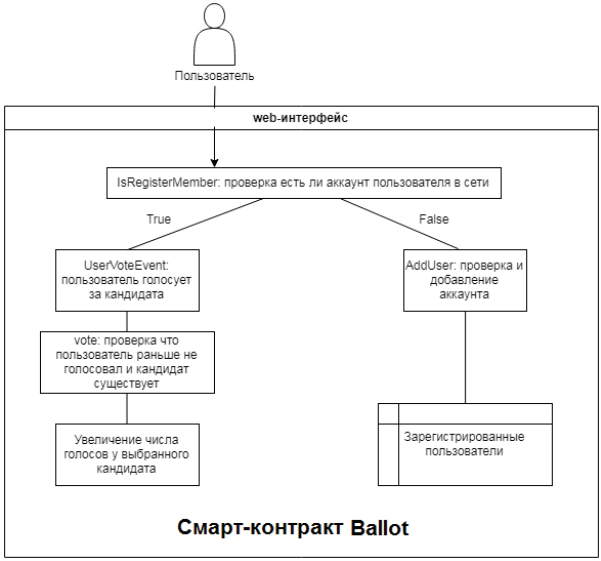

Рис. 5. Схема работы смарт-контракта Ballot

Рассмотрим смарт-контракт подробнее. Когда пользователь заходит на сайт вызывается функция IsRegisterMember, она проверяет, есть ли пользователь в тестовой сети. Если его нет, вызывается функция AddUser и плагин MetaMask предлагает пользователю пройти регистрацию.

После прохождения регистрации пользователь добавляется в сеть и снова вызывается функция IsRegisterMember. После этого пользователя перенаправляет на форму приложения (рис. 6).

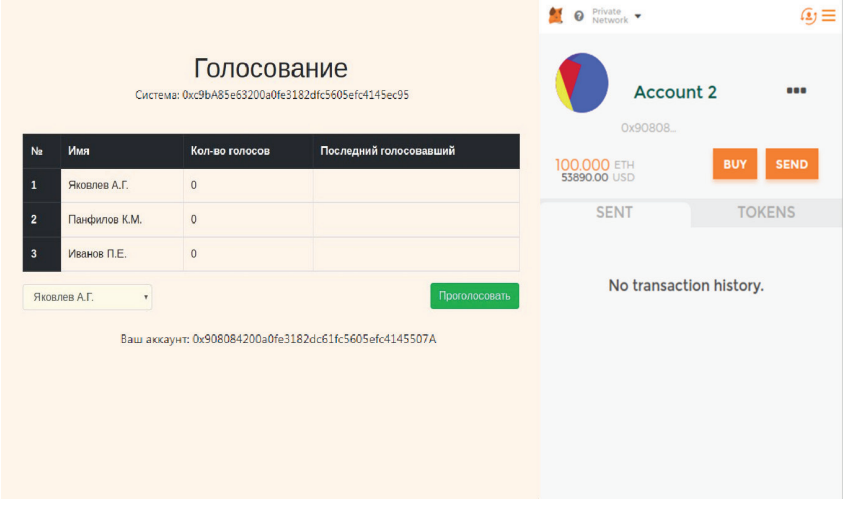

Рис. 6. Интерфейс приложения и плагин MetaMask

После выбора пользователем кандидата и нажатия кнопки “Голосовать” происходит UserVoteEvent и вызывается функция vote. Затем пользователь должен подтвердить транзакцию (рис. 7).

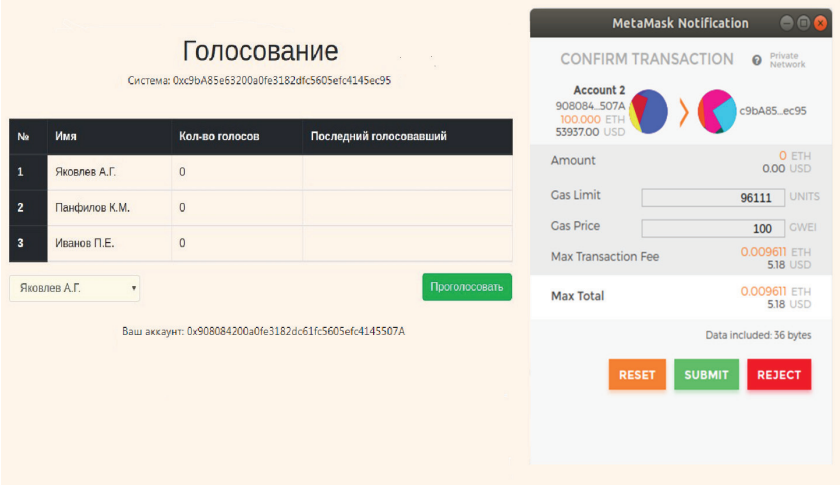

Рис. 7. Подтверждение транзакции

После подтверждения транзакции и проверки, что данный пользователь ещё не голосовал, и такой кандидат существует количество голосов выбранного кандидата увеличится на 1. Также в поле “Последний голосовавший”, выбранного кандидата, появится номер аккаунта голосовавшего. (рис. 8).

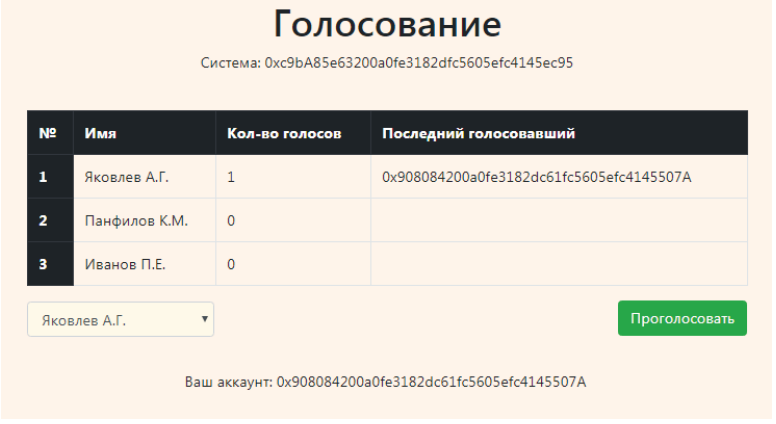

Рис. 8. Результат работы программы

В результате работы было создано децентрализованное приложение, осуществляющее функционал голосования. Приложение предоставляет наглядную информацию о совершенных транзакциях и выполнении сценария смарт-контрактов. Также был подобран и разобран инструментарий необходимый для создания приложения, отличающийся ненагруженным интерфейсом и легкостью написания кода.

СПИСОК ЛИТЕРАТУРЫ

1. С.А. Равал, Децентрализованные приложения / С.А. Равал. – Санкт-Петербург: Питер, 2017;
2. М.С. Свон Блокчейн схема новой экономики / М.С. Свон. – Москва: Олимп-бизнес, 2015;
3. Pedro Franco. The Blockchain // Understanding Bitcoin: Cryptography, Engineering and Economics – John Wiley & Sons, 2014;

Артем Генкин, Алексей Михеев. Блокчейн. Как это работает и что ждет нас завтра. – М.: Альпина Паблишер, 2017;

Melanie Swan. Blockchain: Blueprint for a New Economy. – O'Reilly Media, Inc., 2015;

Andreas M. Antonopoulos. Mastering Bitcoin: Unlocking Digital Cryptocurrencies – O'Reilly Media, Inc., 2014;

Roger Wattenhofer. The Science of the Blockchain – CreateSpace Independent Publishing Platform, 2017.