

Обеспечение цифровой демократии при помощи публичного блокчейна со смарт – контрактами

*Стефанова Н.А., к.э.н., доцент, заместитель заведующего кафедрой
«Цифровая экономика»*

*Палкин Н.А., студент кафедры
«Цифровая экономика»*

*ФГБОУ ВПО «Поволжский государственный университет
телекоммуникаций и информатики»*

e-mail: palkin-wes@yandex.ru

Россия, г. Самара

В демократических государствах нередко встаёт вопрос о справедливых выборах главы государства. В данной статье предложен метод осуществления цифровой демократии, в рамках которой рассматривается возможность использования блокчейн – платформы, которая не только позволит проводить тайное и контролируемое голосование, но и позволит снизить расходы на организацию выборов.

Избирательный процесс является одной из форм реализации конституционного права граждан избирать и быть избранными в государственные и муниципальные органы власти, что представляет важнейшую процедуру осуществления суверенной воли народа. Избирательный процесс регламентируется процессуальными нормами избирательного права. На сегодняшний день, с помощью информационных технологий, стало возможным реализовать электронные выборы, с прозрачностью результатов голосования, а также с предельной защищенностью информации от фальсификации.

Лаборатория Касперского долгое время занималась разработкой проекта, целью которого являлось – создание возможности проведения электронных голосований. Осенью 2017 года международная компания заявила о выходе «Polys» – инновационной платформы электронного голосования [1]. Платформа построена с использованием технологий блокчейн Ethereum (далее Эфир). В ней для подсчета голосов используется тщательно продуманный алгоритм, который исключает фальсификацию голосов [2].

Платформа с использованием Эфира может использовать смарт-контракты. Благодаря децентрализованным системам, которые создаются смарт-контрактами, станет возможным проверка учёта голосов. При этом каждый гражданин также сможет проверить корректность учёта его голоса.

Посредством данной технологии итоги выборов, а также вся информация, касающаяся процесса выборов, хранятся в информационных блоках на устройствах всех участников процесса. Такой способ позволит защитить информацию от взлома, чтобы внести изменения в блок, необходимо будет взломать всю цепочку блоков. Все блоки зашифрованы с

использованием математических алгоритмов. Шифрование позволяет делать голосование анонимным, а также даёт возможность скрывать промежуточные результаты подсчётов, итоги голосования становятся доступны всем, только после полного подсчёта.

Блокчейн – непрерывная и последовательная цепочка информационных блоков, которые выстраиваются по определённым правилам. Безопасность технологии заключается в том, что для осуществления сделки существует неизбежный процесс – каждый блок цепочки проверяется друг за другом, у всех блоков должны совпадать подпись и формат. Для защиты блоков от подделки, копии цепочек блоков хранятся независимо друг от друга на множестве компьютеров, в каждом новом блоке хранится информация о предыдущем.

На базе блокчейна созданы надстройки, которые позволяют фиксировать договорённости между субъектами и отслеживать исполнение описанных договоренностей – так называемые «смарт-контракты». Смарт контракт – электронный контракт или алгоритм, который прописывает все действия, которые должна совершить одна и другая сторона для получения желаемого результата [3].

Блокчейн Ethereum стал первым, где возможно программировать универсальные контракты. Подписание смарт-контракта происходит примерно так же, как подписываются транзакции. Смарт-контракты создаются на формальном языке программирования. После исполнения своих обязательств одной стороной, вторая сразу же получает полагающуюся за исполнение обязательств оплату. На базе блокчейна Ethereum был создан «токен» – некоторая единица учёта, не являющаяся криптовалютой, но предназначенная для представления цифрового баланса. Токен можно перемещать с блокчейн-адреса на другой. Фактически, токен можно представлять, как жетон, который один владелец может передавать другому, такие транзакции описаны с помощью смарт-контрактов.

Организация избирательного процесса при помощи блокчейн-технологии на платформе Эфира выглядит следующим образом.

1. Каждый избиратель должен будет получить индивидуальный Эфир-адрес. Это следует организовать в два этапа – для текущих избирателей и для тех, кто ими становится по мере взросления. Для получения такого адреса можно использовать инфраструктуру Многофункциональных центров (МФЦ) или сайта Госуслуг.

2. Избиратели направляются в МФЦ и получают инструкцию о том, как завести Эфир-адрес, где хранить приватные ключи, как проводить транзакции. При необходимости сотрудник МФЦ оказывает помощь.

3. Избирателям может быть представлено два способа голосования на выбор: с помощью установки мобильного приложения, либо через персональный компьютер используя web-сайт. Исходные коды приложения и всех смарт-контрактов должны лежать в открытом репозитории, чтобы любой мог сделать проверку.

4. При запуске голосования по определённому вопросу (референдум, выборы и т. д. на любом уровне) для всех избирателей, кто имеет право участвовать в соответствующем избирательном процессе, эмитируются токены для соответствующей избирательной компании – по одной единице каждому. Каждому участнику выборов присваивается 1 токен, который он должен переслать до окончания голосования на адрес смарт-контракта, подсчитывающего голоса. Токен будет выполнять роль голоса. Входным цензом за участие в выборах, блокчейн будет требовать комиссию для проведения сделки. Это можно предусмотреть и выдавать криптовалюту достаточную для совершения транзакции вместе с токеном.

На выборы в 2018 году было выделено около 17,69 млрд рублей. Без учета расходов на предвыборные кампании и рекламу, только для оплаты комиссионного сбора государство может тратить около 168 тыс. рублей, если каждому из 120 000 000 человек способному принимать участие в выборах, будет выдано 0,0000001 эфириум для оплаты комиссионного сбора, при курсе 1 ETH = 14 263,54 RUB. Такие расходы будут являться незначительными, по сравнению с расходами на аренду помещений, их обустройство, расходы на транспорт, по всей стране.

Также имеются аналоги зарубежных компаний использовавшие технологии блокчейн. Считается, что первыми в мире электронные выборы были проведены 7 марта 2018 года в Западной Африке, в Сьерра-Леоне. Платформу для голосований предоставила швейцарская компания Agora. В своей платформе, Agore не используют криптовалюты, в основе лежит частный блокчейн. Только специальные органы могут вносить записи в реестр. Такими уполномоченными органами были – Красный Крест, Высшая техническая школа Лозанны и Университет Фрайбурга.

Процесс электронного голосования с помощью «Агора» состоит из шести отдельных шагов, которые вместе обеспечивают криптографически проверяемое решение для голосования, которое заслуживает доверия избирателей.

Выборы на платформе Агоры проходят в соответствии со следующими шагами:

1. Конфигурация: органы управления создают событие выборов;
2. Голосование: избирателями заполняются бюллетени, затем отдают свои бюллетени в пункты приёма;
3. Анонимизация: сеть Агоры зашифровывает все избирательные бюллетени, что позволяет сделать их уникальными;
4. Расшифровка: после завершения сбора бюллетеней, сеть Агоры занимается расшифровкой;
5. Подсчет итогов: подсчитываются все голоса;
6. Аудит: Наблюдающие за процессом делают свой обзор, подтверждающие достоверность результатов выборов.

Инновационная платформа, созданная Лабораторией Касперского, несомненно имеет ряд конкурентных преимуществ перед швейцарской компанией. Основным преимуществом является возможность проведения

онлайн-голосований, без использования бюллетеней. Так же, «Polys» позволяет реализовывать процесс голосования не на частных блокчейн, напротив, предлагаемая система – с открытым доступом для всех.

С 2017 года мы вступаем в интереснейший период реального продвижения блокчейн-технологии на рынок e-Government.

Обеспечение цифровой демократии при помощи публичного блокчейна со смарт – контрактами стало возможным уже сегодня, барьером для внедрения инновационной платформы электронного голосования, является необходимость вносить изменения в текущее законодательство, чтобы оно позволило принять внедрение новейших технологий. Как результат, внедрение подобной системы высвободит огромное количество ресурсов. По приблизительным оценкам, организация общенациональных выборов по такой технологии значительно дешевле.

Использованные источники

1. Kaspersky.ru [Электронный ресурс] / Выпуск инновационной платформы электронного голосования. Режим доступа: свободный
2. Polys.me [Электронный ресурс] / Технология. Режим доступа: свободный
3. Mining-cryptocurrency.ru [Электронный ресурс] / Смарт-контракты. Режим доступа: свободный.

Контактный телефон: +79608398133