

Обеспечение цифровой демократии при помощи публичного блокчейна со смарт-контрактами

Бритвина Е. Н. (britvina.elena@gmail.com)

Душкин Р. В. (roman.dushkin@gmail.com)

В современном мире крайне остро встаёт вопрос обеспечения возможности для каждого дееспособного гражданина выразить свою волю на плебисцитах любого уровня, на которых он имеет право участия. В предлагаемой статье описывается один из методов обеспечения цифровой демократии, в рамках которой плебисциты организованы на блокчейн-платформе, что позволяет осуществлять тайное и проверяемое голосование.

Введение

Избирательный процесс выступает в качестве одного из форматов реализации субъективного и объективного избирательного права, что представляет важнейшую процедуру осуществления народовластия. Организация избирательного процесса в основном регламентируется процессуальными нормами избирательного права, а сам избирательный процесс — это последовательность событий, определяемых на законодательном уровне. Современные технологии, реализующие электронное голосование, могут помочь обеспечить прозрачность и проверяемость результатов избирательного процесса и значительно снизить издержки на его реализацию.

Первое электронное интернет-голосование в России состоялось в 2008 году в городе Новомосковск Тульской области [1]. Затем в 2009 году электронные выборы состоялись в городе Урюпинске Волгоградской области [2] и в 2010 году в городе Одинцово Московской области [3].

За последние 10 лет инфраструктура информационно-коммуникационных платформ, поддерживающих различные бизнес-процессы — государственные, финансовые и другие — столкнулись с возросшими требованиями к обеспечению быстродействия, доступности, безопасности и надёжности. В ноябре 2017 года российская компания Лаборатория Касперского анонсировала свою платформу для голосования с помощью блокчейн-технологий [5]. Платформа построена на основе блокчейна *Ethereum* (далее — «Эфир») [6]. Эта технология гарантирует неизменность результатов голосования, защиту от атак и доступность информации для валидации любому лицу.

И уже летом 2018 года в швейцарском городе Цуг было проведено тестирование ИТ-инфраструктуры для выборов на блокчейне — технологии, позволяющей обеспечить вышеуказанные требования на самом современном и высоком уровне. Результаты тестирования показали, что 30 % населения города Цуг проголосовали с помощью технологии блокчейн. Пилотный проект был признан в целом успешным как самими избирателями, так и властями города.

Далее в этой статье рассматриваются составные компоненты системы электронного голосования на основе платформы Эфир и вариант её интеграции в избирательный процесс.

Кратко о криптоинструментарии

Все определения в этом разделе даны в соответствии с источником [7]. Приведённые определения помогут лучше понять предлагаемую систему голосования на базе Эфира.

Блокчейн — это журнал, в котором каждая запись, кроме первой, содержит специальную хэширующую последовательность, некоторым образом идентифицирующую предыдущую запись. Чаще всего, блокчейн представляет собой реестр, распределённый по множеству баз данных. В каждой записи блокчейна, кроме первой, есть специальное служебное поле, которое содержит идентификатор предыдущей записи, за счёт чего выстраивается связанная цепочка — каждая новая запись ссылается на предыдущую.

Важно, что на базе блокчейна созданы надстройки, которые позволяют фиксировать договорённости между субъектами и отслеживать исполнение описанных договорённостей — так называемые «смарт-контракты». *Смарт-контракт* — это программная сущность, которая хранится в блокчейне. Первым блокчейном, где стало возможно программировать универсальные контракты стал блокчейн Эфира. Именно поэтому с 2013 года Эфир стал популярен, и сегодня токен этого блокчейна ETH является второй по капитализации криптовалютой. В блокчейне Эфира можно исполнять программный код на тьюринг-полном языке программирования Solidity, а это значит, что после подписания смарт-контракта сторонами его исполнение гарантируется инфраструктурой блокчейна. Подписание смарт-контракта происходит примерно так же, как подписываются транзакции. Смарт-контракты составляются на формальном языке программирования, а не на казуистическом языке юристов. Если одна сторона исполняет свои обязательства, вторая сразу же получает полагающуюся за исполнение обязательств оплату.

Токен — некоторая единица учёта, не являющаяся криптовалютой, но предназначенная для представления цифрового баланса, своеобразный «заменитель ценных бумаг» в криптовалютном мире. Токены можно перемещать с блокчейн-адреса на другой. Фактически, токен можно представлять себе как жетон, который один владелец может передавать другому. Само собой разумеется, что в рамках блокчейна Эфира движение токенов описывается при помощи смарт-контрактов.

Как организовать избирательную систему

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

1. Каждый избиратель должен получить индивидуальный Эфир-адрес. Это следует организовать в два этапа — для текущих избирателей и для тех, кто ими становится по мере взросления. Для получения Эфир-адреса можно использовать инфраструктуру Многофункциональных центров (МФЦ) или сайта Госуслуг.
2. Текущие избиратели направляются в МФЦ и получают инструкцию о том, как завести Эфир-адрес, где хранить приватные ключи, как проводить транзакции и т. д. При необходимости сотрудник МФЦ оказывает помощь, но необходимо организационный

механизм, чтобы никто не мог получить приватный ключ от Эфир-адреса, кроме самого избирателя.

3. По достижении совершеннолетия молодой избиратель получает такую же инструкцию, но уже при осуществлении какого-либо обязательного регистрационного действия (например, получения общегражданского паспорта).
4. Для голосования каждый избиратель должен установить себе мобильное приложение, либо воспользоваться специальным web-сайтом, либо плагином для браузера (типа MetaMask), чтобы осуществлять свои избирательные права. Исходные коды приложения и всех используемых в процессе этого смарт-контрактов должны лежать в открытом репозитории, чтобы любой мог провести аудит. Эти сервисы (приложение и веб-сайт) предоставляют простой интерфейс доступа к смарт-контрактам, чтобы избирателям не нужно было дополнительно изучать нативные интерфейсы блокчейна.
5. 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 одному для каждого. Каждому избирателю отправляется 1 токен, который он должен переслать не позднее срока окончания голосования на адрес смарт-контракта, подсчитывающего голоса. Каждый токен — 1 голос. За отправку токена взимается плата за транзакцию. Блокчейн Эфира потребует от избирателя самостоятельно заплатить небольшую цену за участие в избирательном процессе. Это является входным цензом за участие в политике. Но можно предусмотреть возможность вместе с токеном для голосования отправлять немного криптовалюты для оплаты комиссионного сбора.

В чем же плюсы и минусы подобной системы?

Очевидный минус — высокий порог входа в технологию, поскольку необходимо обучать людей. Но, к примеру, 10 лет назад платёжные карты были технологической новинкой, не говоря уже о современных системах оплаты с помощью мобильных телефонов. В добавление, сложно сравнивать оффлайн-систему с электронной системой голосования. У оффлайн-системы уже выверены и обкатаны все процедуры риск-менеджмента: от отключения электричества на избирательном участке до любого форс-мажора. Хотя, как показывает практика, электронные системы часто более предсказуемы и безопасны, чем люди, задействованные в оффлайн-процессах.

Плюсов у такой системы значительно больше:

- Во-первых, осуществление прозрачных выборов с валидируемыми результатами. Любой человек может проверить все транзакции и убедиться, что голоса подсчитаны корректно. Доверие обеспечено самим блокчейном Эфира.
- Во-вторых, систему можно использовать на любом уровне — от дома, села или муниципалитета до общемирового референдума.
- В третьих, непосредственная демократия по любому вопросу, без затрат. Плебисциты можно устраивать хоть каждый день.
- И последнее, наиболее важное — чётко обоснованные результаты, которые невозможно оспорить. Никаких оранжевых революций, всё в блокчейне.

Выводы

Безусловно, для внедрения подобной системы потребуется изменение текущего законодательства на всех уровнях, которые необходимы для того, чтобы оно позволило принять все необходимые технологические новинки.

Предложенная идея позволяет реализовывать процесс голосования не на частных блокчейнах, что само по себе ставит под вопрос прозрачность процесса. Напротив предлагаемая система — с открытым доступом для всех.

Как результат, внедрение подобной системы высвобождает огромное количество ресурсов. По приблизительным оценкам, организация общенациональных выборов по такой технологии на 2 — 3 порядка дешевле, даже если каждому избирателю отправлять эфир для оплаты комиссии.

Источники информации

1. <http://polit.ru/news/2008/10/13/evote/>
2. <https://v1.ru/text/gorod/153717.html>
3. <http://odintsovo.org/election-2010/result.asp>
4. <https://business-swiss.ch/2018/06/cug-jelektronnoe-golosovanie-po-blokchejn>
5. https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-introduces-electronic-voting-system
6. <https://www.ethereum.org>
7. <http://teleschool.me/01>