Л. Х. Тагирова, Е. В. Остапчук, Т. И. Паюсова

Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ГОЛОСОВАНИЯ В СЕТИ ETHEREUM

Аннотация. В статье рассматриваются проблемы существующих систем голосования и возможные способы их решения с помощью технологии блокчейн.

Ключевые слова: голосование, системы голосования, блокчейн, blockchain, Ethereum, цифровая экономика.

Многие сервисы переходят в режим онлайн: оплата различных услуг, покупка товаров в онлайн магазинах, онлайн-образование и т.д., так как это значительно сокращает расходы владельцев бизнеса, а также время, необходимое для выполнения того или иного действия. Но голосование по-прежнему проводится в избирательных пунктах с условием обязательного присутствия.

Существующие системы голосования имеют ряд недостатков:

1. Централизованная обработка результатов;
2. Невозможно проверить, был ли засчитан голос;
3. Возможность вносить изменения в базу данных;
4. Большие затраты на организацию голосования (помещения, бумага).

Из-за централизованности обработки голосов избиратели не могут контролировать процесс голосования, проверять правильность подсчета голосов и узнавать не были ли подделаны голоса участников голосования. Применяя технологию блокчейн, процесс голосования становится прозрачным, то есть по окончании голосования участник может проверить, был ли засчитан его голос, не изменился ли его выбор.

Всё что требуется избирателю – иметь смартфон/компьютер и доступ в сеть Интернет. Перед самим голосованием участнику необходимо зарегистрироваться на платформе голосования и подтвердить свою личность. Таким образом, участнику голосования не нужно приходить в определенный день в назначенное место.

Актуальность данной работы обусловлена следующими проблемами в существующих системах голосования:

1. Современные системы голосования проводят централизованную обработку результатов;
2. Необходимость физического присутствия голосующего в пункте голосования;
3. Отсутствие единого цифрового решения для систем голосования различного назначения.

На данный момент есть несколько решений, позволяющих проводить голосования на блокчейне. Проект Agora начал разрабатываться с 2015 года в Швейцарии на платформе Ethereum. Данный проект применялся в президентских выборах в Сьерра-Леоне. Компания Agora выступала в роли международного наблюдателя на выборах и проводила независимый подсчет голосов путем ручного ввода голосов в блокчейн [1].

В России создан проект на блокчейне Polys. Проект представляет собой систему с открытым исходным кодом. Polys предлагает развернуть приватный блокчейн в своей IT-инфраструктуре. Преимуществом данного решения является то, что только та компания, которая развернет у себя приватный блокчейн, будет иметь доступ к данным голосования и никто другой. Однако сам избиратель может удостовериться, что его выбор учтен. С помощью системы уже проголосовали десятки тысяч избирателей, в частности студенты Высшей школы экономики и Тюменского государственного университета на выборах в студенческие организации [2].

Целью данной работы является разработка децентрализованного приложения “Голосование” в сети Ethereum.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Изучить текущие системы голосования, их особенности, уязвимости и преимущества, определяемые предметной областью;
2. Изучить средства и методы безопасной разработки смарт-контрактов
3. Разработать безопасный смарт-контракт в сети Ethereum
4. Разработать безопасный веб-интерфейс для голосования

Традиционное голосование требует больших ресурсов для организации процесса голосования, в том числе печати бюллетеней, аренды помещений, человеческих ресурсов и рекламных кампаний для увеличения явки избирателей. Также традиционная система голосования не гарантирует точности подсчетов результатов, так как учитывая человеческих фактор, некоторые голоса могут остаться не засчитанными.

Интернет-голосование может увеличить явку избирателей, не требует огромных вложений на организацию процесса каждого голосования, необходимо потратить на весь процесс минимум времени. Недостатком является то, что такая система будет привлекать интерес со стороны лиц, которые будут пытаться взломать данную систему, поскольку обработка всех результатов также осуществляется централизованно.

Блокчейн голосование позволяет решить проблемы предыдущих систем голосования. Процесс голосования будет представляться в виде обычной блокчейн транзакции. Любой человек, который прошел идентификацию и получил право голоса, может отправить транзакцию в сеть Ethereum, и транзакция будет содержать его выбор, который благодаря криптографической защите не будет доступен для изменения третьим лицам. Также блокчейн позволяет каждому участнику проверить, был ли его голос верно засчитан.

Блокчейн является децентрализованной системой. Благодаря децентрализации люди не нуждаются в помощи посредников, например, для

совершения сделки. Человек может провести любую P2P (peer-to-peer, равный к равному) транзакцию, и в данной ситуации не будет третьего лица, который являлся бы гарантом платежа, так как система сама гарант, обеспечивающий безопасность.

Блокчейн представляет собой два связанных друг с другом объекта (рис. 1): блока и цепочки. Блоком называют цифровую информацию, которая хранится в открытой базе данных (цепочке). В контексте голосования блоки содержат транзакции с информацией о том, кто и за кого проголосовал [3]. Один блок может включать в себя определенное количество транзакций. По достижении определенного числа транзакций, блок добавляется в блокчейн и становится общедоступен.

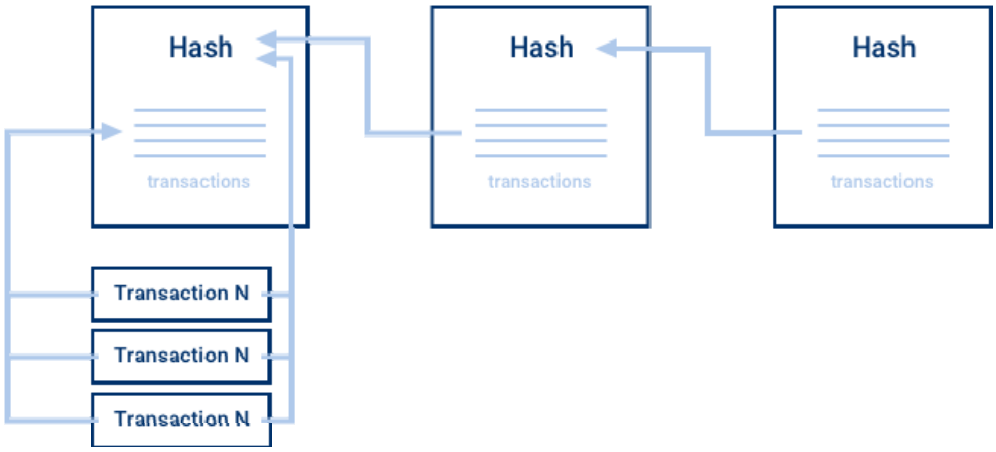

Рис. 1. Структура блокчейна.

Каждый участник (узел) данной сети обладает копией цепочки блоков, таким образом становится невозможным внести изменения в опубликованные ранее блоки. Блокчейн обеспечивает безопасность тем, что каждый новый блок добавляется линейно и хронологически. С помощью такого метода возникают сложности с изменением данных в предыдущих блоках, так как каждый блок хранит свой хэш (цифровой отпечаток) и хэш предыдущего блока.

С помощью блокчейна избирательный процесс станет прозрачным, позволит сократить количество необходимого для выборов персонала, станет доступным каждому, так как для голосования требуется только

телефон/ноутбук/планшет или другие устройства с доступом в Интернет, а также обеспечит мгновенный результат.

Онлайн голосования позволяют устранить возможные ошибки при подсчете голосов, увеличить явку избирателей, так как избиратель может по определенным обстоятельствам не прийти/не успеть на процесс голосования. Онлайн голосование позволяет решить данную проблему путем создания возможности для регистрации/авторизации субъекта в системе голосования. Данная платформа применима не только для политических голосований, но также ее можно использовать, например, для выбора старосты в школе, руководителя отдела, ответственного по жилому дому, спортивного судейства, суда присяжных и др.

Особенностью онлайн голосования является его прозрачность, то есть каждый избиратель вправе проверить, был ли его голос засчитан и правильно ли были подсчитаны голоса.

При разработке данной системы необходимо предусмотреть проверку, направленную на то, чтобы избиратели не могли голосовать за одного кандидата бесчисленное количество раз. Данная проблема устранима путем создания подсистемы, в которой необходимо регистрироваться перед голосованием с вводом своего документа, удостоверяющего личность. После регистрации субъекту будет присвоен идентификационный номер, с которым субъект имеет право голосовать.

Проблема накрутки пользователей актуальна, если не использовать дополнительной меры подтверждения личности с помощью паспорта. В нашем случае возможность накрутки пользователей сводится к минимуму, так как человеку при регистрации необходимо подтвердить свою личность с помощью дополнительного модуля проверки личности. Данный модуль сверяет фото в паспорте с лицом участника через веб-камеру. Участнику при данной проверке необходимо выполнить, например, поворот/наклон головы.

Открытость блокчейна является недостатком для голосования. Если все голоса будут записываться в блокчейн во время голосования и будут

открыты, то это может повлиять на мнения тех, кто еще не проголосовал. Голосование в большинстве задач должно быть анонимным, и результаты голосования должны быть доступны только после окончания голосования, поэтому в системе будет предусмотрен модуль, обеспечивающий анонимный или неанонимный режимы голосования с использованием шифрования данных.

Архитектура приложения “Голосование” представлена на рис. 2:

1. Изначально голосующему необходимо зарегистрироваться на сайте. Для регистрации требуется ввести паспортные данные (страница с фотографией);

2. Для устранения возможности регистрации с поддельным паспортными данными и накрутки пользователей, голосующий проходит верификацию: с помощью дополнительной проверки через веб-камеру проверяется подлинность голосующего с фото в паспорте;

3. После подтверждения подлинности голосующего, голосующему предоставляется уникальный идентификатор, с помощью которого он может голосовать.

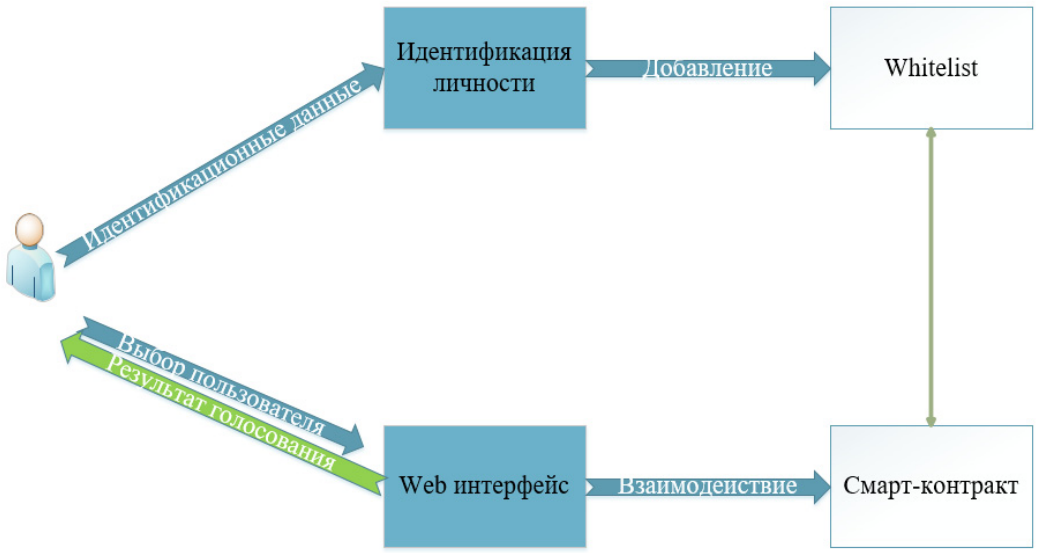

Рис. 2. Архитектура приложения “Голосование”.

Идентификатор добавляется в список, в который записываются все идентификаторы, планирующие голосование. Во время голосования смарт-

контракт обращается этому списку (Whitelist) с целью проверки идентификатора голосующего. Если данный идентификатор есть в Whitelist, тогда голос засчитывается.

Голосующему уникальный идентификатор присваивается только в отношении одного голосования. После окончания голосования все данные о пользователе удаляются. Таким образом, один идентификатор не будет принадлежать только одному голосующему.

Данная работа предусматривает создание конструктора систем голосования с различными опциями и функциями, определяемыми предметной областью голосования. Конструктор может применяться в разных сферах деятельности.

В данной работе в качестве основы программного продукта применяется блокчейн-платформа Ethereum. Ethereum предоставляет возможность не только хранить данные, но и запускать собственные приложения, создавать смарт-контракты, обладает собственной единицей платежа (эфир) и собственный язык программирования для смарт-контрактов (Solidity).

На основе данного блокчейна будет производиться разработка смарт-контрактов. Тестовая сеть позволяет производить отправку определенных транзакций, тестирование контрактов, не используя действующую сеть Ethereum. Монеты тестовой сети не имеют ценности.

Перед запуском смарт-контракта необходимо написать код контракта, проверить его в тестовой сети, определить слабые места кода и устранить их. После всех проверок контракта будет осуществлен запуск контракта в настоящую сеть Ethereum. Стоит отметить, что код смарт-контракта после публикации в сети невозможно изменить.

Изучение смарт-контрактов проводится с помощью ресурса «CryptoZombies». В нем описаны все тонкости смарт-контрактов, теория и практика. Создание веб-интерфейса голосования производится с помощью

JavaScript-библиотеки ReactJS. Данная библиотека выбрана за ее высокую скорость работы и «реактивное» обновления данных.

На данный момент есть несколько решений, позволяющих проводить голосования на блокчейне. Проект Agora начал разрабатываться с 2015 года в Швейцарии на платформе Ethereum. Данный проект применялся в президентских выборах в Сьерра-Леоне. Компания Agora выступала в роли международного наблюдателя на выборах и проводила независимый подсчет голосов путем ручного ввода голосов в блокчейн [2].

В России создан проект на блокчейне Polys. Проект представляет собой систему с открытым исходным кодом. Polys предлагает развернуть приватный блокчейн в своей IT-инфраструктуре. Преимуществом данного решения является то, что только та компания, которая развернет у себя приватный блокчейн, будет иметь доступ к данным голосования и никто другой. Однако сам избиратель может удостовериться, что его выбор учтен. С помощью системы уже проголосовали десятки тысяч избирателей, в частности студенты Высшей школы экономики и Тюменского государственного университета на выборах в студенческие организации [3].

В заключение хотелось бы отметить то, что технология блокчейн стремительно внедряется не только в политическую сферу, но также и в область медицины с целью безопасного хранения медицинских карт пациентов, в банках (блокчейн позволяет избежать проблемы работы банков только в определенные часы), в платформах, осуществляющих резервное копирование данных и т.д. Перспективы использования блокчейн огромны как для отдельных областей, так и для обеспечения программы цифровой экономики РФ в целом.

СПИСОК ЛИТЕРАТУРЫ

1. CoinDesk. The Sierra Leone Vote: What We Got Wrong? // URL: https://www.coindesk.com/ethereum-core-developers-debate-benefits-of-more-frequent-hard-forks (дата обращения: 13.04.2019)

2. Голосование перемещается в интернет // URL: https://polys.me/ru/blog/article/voting-moves-to-internet (дата обращения: 13.04.2019);
3. Д. Кобылинский. Как создать систему электронного голосования на блокчейне? // URL: https://habr.com/ru/post/340342/ (дата обращения: 13.04.2019)
4. Panda Security. Влияние блокчейн на информационную безопасность // URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/342639.php (дата обращения: 2.04.2019);
5. Sagar Shah, Qaish Kanchwala, Huaiqian Mi. Block Chain Voting System // URL: https://www.economist.com/sites/default/files/northeastern.pdf (дата обращения: 11.04.2019);
6. Christian Meter. Design of Distributed Voting Systems // URL: https://arxiv.org/pdf/1702.02566.pdf (дата обращения: 11.04.2019);
7. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. No2 (254). URL: https://cyberleninka.ru/article/n/pravo-i-tsifrovizatsiya-novye-vyzovy-i-perspektivy (дата обращения: 11.04.2019).