

РАЗРАБОТКА СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннотация. В статье представлена разработка web-приложения для проведения электронного голосования с использованием технологии «блокчейн».

Ключевые слова: прикладные информационные технологии, электронное голосование, тайное голосование, блокчейн.

В наше время большое внимание уделяется процедурам голосования по самым разным вопросам [1]. С развитием общества старые методы голосования с использованием бюллетеней уже не кажутся рациональными и эффективными, и на смену им приходит новый способ - электронное голосование. Благодаря внедрению электронного голосования, достигаются следующие цели:

- ☐ участникам предоставляется возможность голосовать дистанционно;
- ☐ процесс голосования значительно упрощается;
- ☐ сокращаются суммарные затраты на проведение голосования;
- ☐ ускоряется процесс подсчета голосов.

Однако электронное голосование имеет свои недостатки, среди которых наблюдаются сложности в обеспечении анонимности избирателей, возможности вброса или фальсификации голосов. Благодаря технологии «блокчейн» можно решить данные проблемы и создать новый безопасный механизм голосования.

Основная цель работы сосредоточена на создании web-приложения с использованием технологии «блокчейн», для проведения любых типов голосования, например, таких как: выборы акционеров, общенациональные выборы местных органов власти, выбор необходимого функционала для мобильного приложения и так далее.

В процессе разработки web-приложения необходимо выявить параметры, которым должна соответствовать создаваемая система:

1. целостность: система гарантирует, что ни один голос не будет изменен во время избирательного процесса;
2. авторизованность: отдать свой голос могут только авторизованные пользователи, причем только один раз, не имея возможности для многократного голосования;
3. устойчивость: системе необходимо выдерживать большую нагрузку и уметь быстро обрабатывать получаемые запросы [2];
4. анонимность: личность избирателя не должна быть никому известна.

Никто, даже организаторы голосования, не должны иметь возможность получить доступ к личности избирателя ни при каких условиях.

Все указанные параметры можно реализовать с использованием технологии «блокчейн», представляющей собой децентрализованную базу данных. Информация в такой базе хранится в блоках, выстроенных в одну цепочку и содержащих данные обо всех совершённых когда-либо операциях. Структура «блокчейна» показана на рисунке 1.

Первый блок в цепочке — первичный блок — рассматривается как отдельный случай, так как у него отсутствует родительский блок. Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. [3] Транзакции — это реальные данные в блочной цепи, которые полностью публичны. Когда пользователь пытается совершить транзакцию, система проверяет ее, прежде чем добавлять в цепочку. Таким

образом, проверка предотвращает двойное или неполноправное использование голосов.

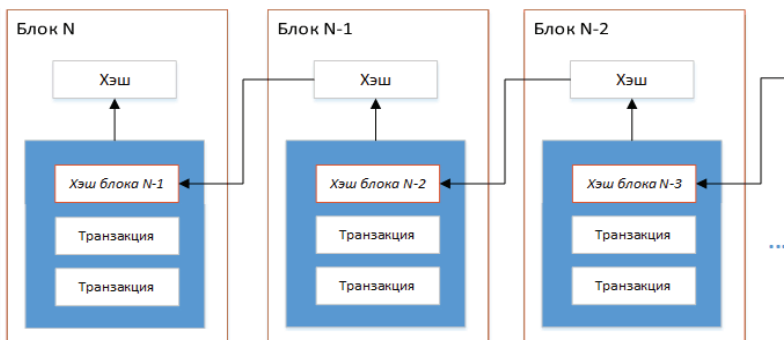


Рис. 1. Структура «блокчейна»

Платформа Waves обеспечивает внедрение технологии «блокчейн». Waves — это блок-система, с полностью открытым исходным кодом. Система является децентрализованной и «прозрачной» [4]. Каждый блок данной платформы может обрабатывать около ста транзакций в минуту, что обеспечивает возможность проведения крупномасштабных голосований. Транзакцией считается перевод токена (голоса) из одного кошелька в другой.

К основным возможностям разрабатываемого web-приложения относятся:

☐ Регистрация. После прохождения регистрации у пользователя создается waves кошелек на который будут приходить токены для голосования.

☐ Создание голосования. Пользователи имеют возможность создавать публичные и приватные опросы. Публичный опрос означает, что при создании голосования, токены данного голосования будут отправлены всем пользователям системы. В приватном голосовании токены направляются заранее выбранной группе пользователей.

☐ Процесс голосования. Для передачи голоса пользователя необходимо отправить на кошелек выбранного варианта waves токен. Суммарное количество waves токенов на кошельке кандидатов обозначает результат голосования.

☐ Возможность проверки своего голоса. Каждый пользователь может узнать, прибыл ли его голос на кошелек кандидата. В личном кабинете пользователя отображены все совершенные им транзакции.

☐ Защита от двойного голосования. Прежде чем транзакции будут добавлены в «блокчейн», они проверяются на предмет того, поступали ли уже токены на данный кошелек от этого пользователя, в рамках проводимого голосования.

☐ Сокрытие промежуточных итогов. Для того, чтобы промежуточные итоги не могли повлиять на решение избирателей, которые еще не проголосовали, было решено скрыть промежуточные результаты. Итог голосования подводится, когда все пользователи проголосовали или, закончилось время для совершения выбора. Однако, так как пользователи видят все транзакции, поступающие на кошелек кандидата, они могут собственноручно посчитать все отданные голоса.

☐ Подсчет голосов. Как только все пользователи, имеющие доступ к голосованию, сделали свой выбор или как только закончилось время для голосования, система суммирует все токены, которые скопились на кошельках кандидатов, и объявляет победителя.

На рисунке 2 представлен алгоритм регистрации выбора пользователя в приватном голосовании. В алгоритме присутствует две основные проверки:

- 1) Доступ пользователя к голосованию. В рамках этого этапа проверяется, что у пользователя имеются необходимые права для выбранного голосования.
- 2) Успешное проведение транзакции. На данном этапе проверяется, что у пользователя достаточно токенов для участия в голосовании и что ранее он не голосовал.

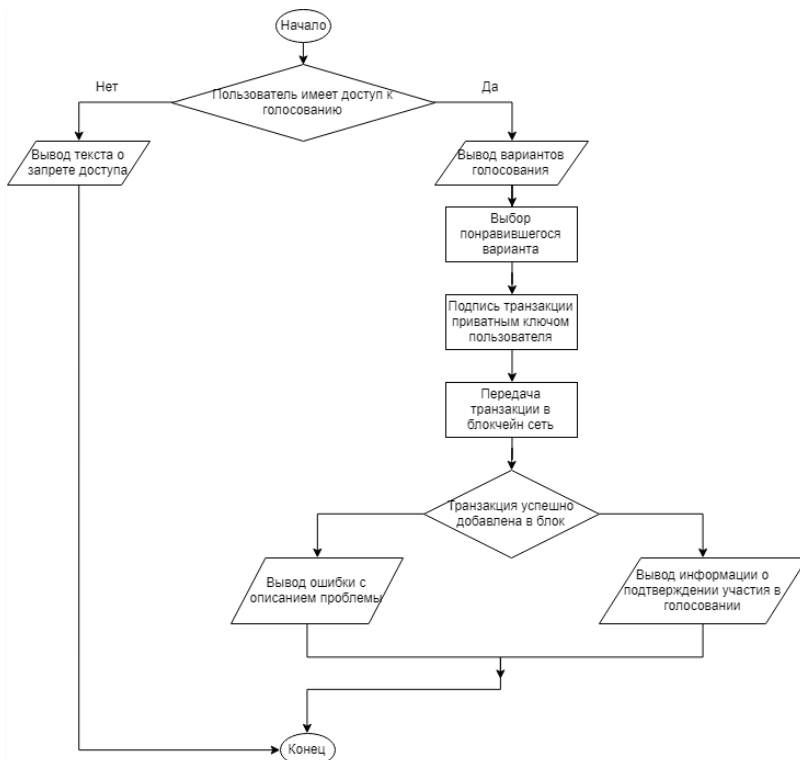


Рис. 2. Алгоритм регистрации голоса пользователя

На рисунке 3 представлена Use case диаграмма пользователя. Пользователь системы может совершать следующие операции: регистрация, авторизация, создание голосования, просмотр списка доступных голосований, просмотр результатов голосования, участие в голосовании, обновление данных профиля.



Рис. 3. Use case диаграмма пользователя

Диаграмма последовательности, показывающая процесс голосования, представлена на рисунке 4.

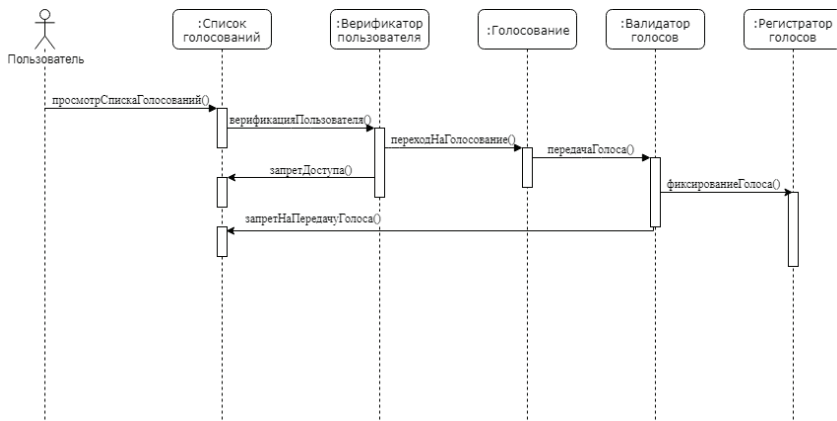


Рис.4. Диаграмма последовательности для процесса голосования

Разработанная система голосования может использоваться при проведении бизнес-семинаров, тренингов, преподавателями, менеджерами по персоналу или маркетингу. Коллективные решения аудитории благодаря системе голосования могут быть приняты быстро и прозрачно, без длительного подсчета голосов, с обеспечением конфиденциальности передачи информации.

Реализованную систему можно применить в качестве системы электронного голосования в любой сфере жизни. В дальнейшем планируется создание отдельного мобильного приложения для корпоративных пользователей, которым необходимо обеспечить дополнительные уровни безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Пескова Ольга Юрьевна, Половко Иван Юрьевич, Фатеева Светлана Владимировна Обзор подходов к организации электронного голосования // Известия ЮФУ. Технические науки. 2014. №2 (151).
2. Денис Баженов [Электронный ресурс]: О высокой нагрузке: <http://bazhenov.me/blog/2012/02/26/highload> (дата обращения: 1.05.2018).
3. Wikipedia [Электронный ресурс]: Блокчейн: <https://ru.wikipedia.org/wiki/Блокчейн> (дата обращения: 14.05.2018).
4. Crypto.by [Электронный ресурс]: Знай свою криптовалюту # WAVES: <http://crypto.by/znajj-svoyu-kriptovalyutu-waves/> (дата обращения: 15.05.2018).