

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.42

Яковчик
Николай Викторович

Мобильное приложение для системы голосования на основе
технологии блокчейн

АВТОРЕФЕРАТ
на соискание степени магистра
по специальности 1-45 80 01 «Системы и сети инфокоммуникаций»

Научный руководитель
Борискевич Илья Анатольевич
кандидат технических наук,
доцент

Минск 2021

КРАТКОЕ ВВЕДЕНИЕ

Значимость инфокоммуникационных технологий в жизни людей достигла небывалых высот. Уже больше половины населения земли имеют доступ к интернету, большая часть пользователей предпочитает выходить в сеть с мобильных устройств. С каждым годом эта тенденция только усиливается. Интернет используется для общения, покупок различных товаров и доступа к услугам. Госорганы по всему миру постепенно переходят на дистанционное обслуживание. Особенно это становится актуально на фоне распространения по миру коронавирусной инфекции, когда посещение мест большого скопления людей чревато проблемами со здоровьем.

Несмотря на вышесказанное, избирательная система многих стран не изменилась за прошедшие десятилетия. Как правило, назначаются определенные дни, в которые избиратель должен явиться на избирательный участок, поставить нужные отметки на бумажном бланке и бросить его в специальную урну, в которой находятся все бюллетени до подсчета результатов. Данный подход имеет ряд недостатков.

Самый очевидный – необходимость физического присутствия на избирательном участке в определенные дни. Это непрактично, т.к. не всегда участок находится в городе постоянного проживания потенциального избирателя, так же возможны случаи проживания их в других странах, что усугубляет ситуацию. В условиях распространения пандемии, даже выход из дома не всегда безопасен. На практике известны случаи, когда бюллетень можно отправлять почтой, но сложно судить о надежности данного подхода.

Возможность голосовать через интернет значительно упростит данный процесс для большого количества людей. Это должно решить описанную выше проблему и в теории увеличить количество голосующих людей. Приложение для мобильного устройства выглядит наиболее подходящим вариантом. В пользу этого решения выступает большая распространённость и доступность мобильных устройств. К тому же, подсчитано, что около 96% населения земли живет в зоне покрытой мобильной сотовой связью.

Вторая проблема – низкая надежность бумажных бюллетеней. Они могут быть повреждены или утеряны. При голосовании на протяжении нескольких дней им требуется охрана, что требует дополнительных финансовых затрат.

Одним из решений описанных проблем может стать разработка системы электронного голосования на основе технологии блокчейн.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования. *Целью* работы является разработка мобильного приложения для системы электронного голосования на основе технологии блокчейн. Для достижения поставленной цели необходимо решить следующие задачи:

- изучить существующие методы и практики проведения избирательных компаний;
- оценить пригодность использования технологии блокчейн в системе электронного голосования;
- разработать систему для голосования на основе технологии блокчейн;
- реализовать прототип мобильного приложения.

Объектом данного исследования является система электронного голосования.

Предметом исследования являются особенности защиты данных в системе голосования на основе технологии блокчейн.

Новизна полученных результатов. В данной работе впервые был применен подход использования полностью децентрализованного приложения для системы электронного голосования.

Положения, выносимые на защиту. На защиту выносятся следующие положения и результаты:

- выявлена необходимая функциональность для разработки мобильного приложения для системы электронного голосования;
- выявлена целесообразность использования технологии блокчейн в качестве платформы для электронного голосования;
- разработан прототип мобильного приложения для системы голосования.

Практической значимостью является возможность использования разработанного приложения при проведении электронного голосования.

Апробация результатов диссертации. Результаты исследований, включенных в данную магистерскую диссертацию были представлены на 57-й научной конференции аспирантов, магистрантов и студентов БГУИР.

Опубликованность результатов исследования. По теме диссертации опубликовано 3 работы в сборниках материалов следующих конференций:

- 57-я научная конференция аспирантов, магистрантов и студентов БГУИР;
- Технические средства защиты информации 2020;
- 56-я научная конференция аспирантов, магистрантов и студентов БГУИР.

Структура и объем диссертации. Настоящая магистерская диссертация разделена на три логические главы по выбранной теме.

Первая глава содержит в себе обзор практик проведения избирательных компаний. А также исследуются сильные и слабые стороны систем электронного голосования. Определяются требования к разрабатываемому приложению.

Вторая глава посвящена технологии блокчейн, как основе для разработки мобильного приложения для системы голосования. Изучена его организационно-техническая структура и возможности смарт-контрактов. Определены преимущества и недостатки технологии. Исследован опыт правового регулирования технологии блокчейн в Республике Беларусь и опыт использования его за рубежом. Проведен сравнительный анализ существующих блокчейн-платформ и выбран оптимальный вариант для целей диссертации.

Третья глава описывает процесс разработки прототипа приложения. Первоначально создан смарт-контракт реализующий логику избирательного процесса и подлежащий загрузке в блокчейн сеть. Исследованы актуальные мобильные платформы с целью определения наиболее актуальной, для которой и следует разрабатывать приложение. Далее изучены существующие подходы к разработке приложений и определен набор инструментов которые нужно использовать в дальнейшем. И в конце реализован прототип приложения для электронного голосования.

Полный объем диссертации – 82 страниц, объем занимаемый иллюстрациями – 2 страница, объем занимаемый таблицами – 0 страниц, объем занимаемый приложениями – 7 страниц. Использовано 63 библиографических источника.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Электронное голосование постепенно начинает использоваться в разных странах мира. В сравнении с традиционным голосование на избирательном участке оно выделяется большей доступностью и возможностью снизить траты на избирательную кампанию а также позволяет не нарушать социальную дистанцию.

Недостатком систем электронного голосования оказалось не уверенность избирателей в том что система работает в соответствии с заявленными параметрами, т.е. отсутствие прозрачности. В качестве решения предложено применить технологию блокчейн как фундамент системы электронного

голосования. Была исследована организационно-техническая структура технологии и определено что по своей концепции блокчейн является подходящим решением. Он гарантирует неизменность вносимых в него данных и абсолютную прозрачность для наблюдателей. Изучен опыт регулирования технологии в Республике Беларусь и зарубежная практика использования, которые показывают большую популярность блокчейна и следовательно доверие к нему.

В качестве блокчейн-платформы выбран Ethereum, основными критериями к выбору которого стало наличие возможности работать со смарт-контрактами, позволяющими реализовать логику избирательного процесса. А также скорый переход платформы на алгоритм консенсуса PoS, позволяющий значительно повысить производительность сети и убрать издержки в виде потраченной энергии на добавление новых блоков цепочки.

Для сохранения анонимности избирателей, предлагается использовать метод слепой подписи адреса блокчейн перед добавлением его в реестр избирателей. А для подписания ключа использовать идентификацию по id-карте.

Был проведен анализ актуальных мобильных платформ на предмет выбора тех для которых следует разрабатывать приложение. Наиболее распространенной является android а следом идет ios. Вместе они охватывают почти весь рынок мобильных устройств поэтому было принято решение разрабатывать приложение под две платформы. Были исследованы подходы разработки приложений и решено использовать кроссплатформенный фреймворк. Он выделяется высокой производительность создаваемых приложений, использованием языка программирования с относительно понятным синтаксисом и популярностью среди разработчиков, что упрощает его дальнейшую поддержку и развитие.

При разработке приложения использовалась концепция чистой архитектуры, подразумевающая разделение приложения на независимые слои, в зависимости от назначения. Данный подход позволил сделать приложение более простым для тестирования а следовательно избежать возможных ошибок в работе. Для связи приложения с блокчейном используется протокол json rpc и библиотека web3dart. Приложение позволяет просмотреть список кандидатов, проголосовать за желаемого и наблюдать актуальную информацию о распределении голосов.

ЗАКЛЮЧЕНИЕ

В ходе работы был исследован опыт применения электронного голосования в разных странах мира. Определено что электронное голосование актуально, и имеет хорошие перспективы развития, способствует росту явки избирателей и иногда позволяет экономить средства. Одним из недостатков электронного голосования является отсутствие доверия к системе, многие ожидают что данные могут быть изменены в ту или иную сторону. Для решения данной проблемы предложено использовать технологию блокчейн в качестве хранилища данных.

Было исследовано устройство блокчейн-сети, определено что в связи с спецификой своей реализации она может гарантировать неизменность вносимых данных и прозрачность для наблюдателей. Многие блокчейн-сети имеют возможность создания смарт-контрактов, программ выполняемых в блокчейне. Смарт-контракты позволяют реализовать логику голосования. Единственной проблемой смарт-контрактов является сложность тестирования, поэтому предпочтительно создание простых методов без сложной логики, для минимизации возможных ошибок. Был изучен опыт применения технологии блокчейн в Беларуси и за рубежом, обширная практика применения которого говорит о популярности технологии и общей доверии к данному подходу. Были исследованы популярные блокчейн-платформы на возможность применения в данной работе. Благодаря ряду преимуществ предпочтение отдано платформе Ethereum. Разработан смарт-контракт на языке Solidity.

Были исследованы актуальные мобильные платформы и определены те для которых следует разработать приложение. Для реализации приложения выбран кроссплатформенный фреймворк flutter, позволяющий сделать приложение запускаемое сразу на двух самых популярных мобильных платформах а также веб версию и версии для персональных компьютеров.

Реализовано мобильное приложение с графическим интерфейсом позволяющее взаимодействовать со смарт-контрактом в блокчейн-сети и выполнять основные функции доступные избирателю, возможность проголосовать и просмотр текущих результатов без необходимости посещать избирательный участок. Использование технологии блокчейн позволило добиться доверия большего процента пользователей и реализовать прозрачность избирательного процесса. Таким образом цель данной работы выполнена, разработан прототип приложения, которое позволяет заменить собой поход на избирательный участок. Результаты голосования из данного приложения сохраняются в блокчейн, для дальнейшей обработки и

мониторинга. При адаптации под конкретные требования, разработанный прототип мобильного приложения можно применять при проведении избирательных компаний различного уровня.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1–А] Яковчик, Н. В. Алгоритмы консенсуса в блокчейн сетях / Яковчик Н. В. // Инфокоммуникации : сборник тезисов докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2020. – С. 116-117.

[2–А] Яковчик, Н. В. Криптография в технологии блокчейн / Н. В. Яковчик // Технические средства защиты информации: тезисы докладов XVIII Белорусско-российской научно – технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Т. В. Борботько [и др.]. – Минск, 2020. – С. 85.

[3–А] Яковчик, Н. В. Оценка производительности блокчейн сетей / Яковчик Н. В. // Инфокоммуникации : сборник тезисов докладов 57-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 19 – 23 апреля 2021 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск : БГУИР, 2021. – С. 79-80.