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

УДК 004.428

БОГУШЕВИЧ
Павел Александрович

ПРОГРАММНОЕ СРЕДСТВО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ПЛАТФОРМЕ ПРИВАТНЫХ БЛОКЧЕЙН СИСТЕМ HYPERLEDGER FABRIC

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра информатики и вычислительной техники

по специальности 1-40 81 01 – Информатика и технологии разработки программного обеспечения

Минск 2020

Работа выполнена на кафедре информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **СКОБЦОВ Вадим Юрьевич,**
кандидат технических наук, доцент кафедры программного обеспечения информационных технологий «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **БУЛОВА Александр Дмитриевич,**
кандидат технических наук, доцент кафедры экономической информатики «Белорусский государственный экономический университет»

Защита диссертации состоится «24» июня 2020 г. года в $10^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. Гикало, 9, копр. 4, ауд. 111, тел. 293-85-91, e-mail: inform@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В настоящее время все более остро стоят вопросы, связанные с корпоративным управлением. Одной из важных сложностей данного процесса является голосования в таких средах. Голосованием акционеры избирают совет директоров, который управляет компанией. Таким образом корпорации принадлежат акционерам, а акционеры реализуют свои права. Такой процесс называется – власть через голосование.

Так как принятие решений в крупных корпорациях несет за собой огромные риски, то остро встает вопрос защиты информации о результатах голосования. В следствие того, что надежность хранения и обработки такой информации обеспечивается частными структурами, у голосующего нет реальной возможности лично обеспечить сохранность данных и, следовательно, защиту своих прав.

С появлением криптовалют, ситуация изменилась. Системы криптовалют позволили пользователям, с помощью других пользователей осуществлять создание и регулирование важнейших процессов при обмене денежными средствами. Данные системы построены на технологии блокчейн. С каждым днем становится все больше криптовалют и вместе с тем, становится все больше отраслей жизни и способов применения технологии полного распределенного реестра.

Одной из самых полезных возможностей блокчейн является обход влияния регулирующих органов и цен на их услуги, а также новый уровень безопасности. С момента создания, криптовалюта «Bitcoin» неоднократно вызывала резонанс и неоднозначные обсуждения, и вместе с тем цена за единицу практически никогда не оставалась стабильной. Однако несмотря на то, что «Bitcoin» не смогла дать человечеству решение всех трудностей, связанных с финансовыми институтами и операциями между ними, вместо этого данная технология показала эффективную работу технологии блокчейн.

За последние годы технология нашла применение в многих прикладных сферах, наиболее интересны из низ следующие:

– авторство и право владения;
– операции с товарами и сырьем;
– управление данными;
– цифровая идентичность;
– проверка подлинности и подтверждение прав доступа;
– организация частного и государственного управления;
– экономика цифровых товаров.

Все это стало возможным благодаря появлению смарт-контрактов, где помимо данных в блокчейн сети находятся также набор функций для этих данных.

Таким образом, использование технологии блокчейн, для обеспечения защиты данных при голосовании, является привлекательным научным исследованием применимым в реальном секторе экономики.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Магистерская диссертация относится к актуальной области современных информационных технологий – использованию технологии приватного блокчейна для решения задачи обеспечения защиты данных голосования. Актуальность работы обусловлена тем, что в настоящее время всё более широкое распространение получают настоящее время остро стоят вопросы, связанные с корпоративным управлением, в частности, реализацией методов управления типа “власть через голосование”. Поскольку принятие решений в крупных корпорациях несет за собой огромные риски, то остро встает вопрос защищенности процесса голосования, личных данных голосующих и результатов голосования. В следствие того, что надежность хранения и обработки такой информации обеспечивается частными структурами, у голосующего нет реальной возможности лично обеспечить сохранность данных и, следовательно, защиту своих прав.

Результаты работы носят как теоретический (комплекс рекомендаций, методик и т.п.), так и практический характер: предложенные смарт-контракт и структура сети могут применяться в системах принятия коллективных решений.

Степень разработанности проблемы

Исследование систем электронного голосования, работающих на основе технологии блокчейн осуществлялось на основе работ российских и белорусских ученых: А.А. Болотова, С.Б. Гашкова, А.Б. Фролова, А.А. Часовских, С.Г. Баричева, М.А. Иванова, а так же зарубежных авторов: А. Миллера, Т. Коннолли, К. Дж. Дейта, А. Салмана, Luc Desrosiers и др.

Одним из недостатков исследований, представленных в современной технической литературе, является рассмотрение проблемы криптографической стойкости алгоритмов, а не масштабируемости использующих их систем.

Предложенное исследование направлено на устранение этого недостатка, в работе целостно рассмотрена задача гибкого обеспечения инфраструктуры и проведения голосования.

Цель и задачи исследования

Целью диссертационной работы является разработка алгоритмов и программного обеспечения для решения задачи проведения электронного голосования с использованием новейших платформ разработки на основе технологии блокчейн.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Определить границы применимости технологии блокчейн в организации и проведении электронного голосования.
2. Разработать архитектуру программного средства электронного голосования на платформе приватных блокчейн систем.
3. Исследовать оптимальный алгоритм консенсуса для нужд голосования.

4. Реализовать ПО для электронного голосования.

5. Провести экспериментальные исследования разработанного программного средства.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 81 01-2012 специальности 1-40 81 01 «Информатика и технологии разработки программного обеспечения».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области использования платформ приватных блокчейн систем в проведении электронного голосования.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в анализе технологий приватных блокчейн систем для решения задачи электронного голосования, разработка программного средства электронного голосования, в предложенном программном средстве используется технология Hyperledger.

Теоретическая значимость работы заключается в детальном анализе технологий и подходов к использованию приватных блокчейнов для систем голосования.

Практическая значимость состоит в приведённом описании, проектировании и разработке программного средства электронного голосования, так же приведено тестирование программного средства и его тестовое использование на примере принятия коллективного решения.

Основные положения, выносимые на защиту

1.Систематизация основных видов электронных голосований, преимущества дистанционного электронного голосования через интернет перед стационарным электронным голосованием.

2. Архитектуры приватных блокчейнов для решения задачи электронного голосования. Анализ их структуры и производительности работы.

3. Обзор Hyperledger для обеспечения гибкой масштабируемой платформы, которая может быть использована для проведения голосования, а также разработка экспериментального программного средства, которое использует фреймворк Fabric для разработки, построения и работы блокчейна.

Апробация диссертации и информация об использовании ее результатов

Основные положения диссертационной работы использовались в разработке системы принятия коллективного решения в корпоративной среде.

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 2 печатных работах. В их числе 2 статьи в рецензируемых журналах

Общий объем публикаций по теме диссертации составляет 8 страниц.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе представлен анализ предметной области, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения.

Во второй главе представлено исследованию основных технологий и платформ, а также возможность их использования для разработки программного средства электронного голосования, приведена сравнительная таблица платформ для разработки децентрализованных приложений.

В третьей главе представлено проектирования программного средства, выбор алгоритма консенсуса, разработана схема сети. Также приведено описание разработки основных модулей программного средства и его тестирование на примере экспериментального использования в качестве средства принятия коллективного решения в корпоративной среде.

В приложении представлены публикации автора и исходный код разработанного программного средства.

Общий объем работы составляет 90 страниц, из которых основного текста – 69 страниц, 24 рисунка на 20 страницах, 2 таблицы на 5 страницах, список использованных источников из 33 наименований на 2 страницах и 3 приложения на 8 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы принятия коллективных решений в корпоративных средах, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, практическая значимость исследований.

В первой главе приведен обзор современного состояния задачи электронного голосования, а также рассмотрены архитектурные особенности основных видов блокчейнов.

Анализ «основополагающей» системы Bitcoin показал пути становления и начала применения в промышленности технологии блокчейн. На примере данной криптовалюты были рассмотрены особенности работы технологии блокчейн, ее возможности и варианты алгоритма нахождения пиринговой сетью консенсуса. В результате было принято решение, что функциональности криптовалюты недостаточно для реализации программного средства электронного голосования, а также что есть необходимость исследовать блокчейны с возможностью хранения в реестре не только данных, но и допустимых над ними операций с возможностью их исполнения.

Обзор блокчейна Ethereum показал расширение возможностей для реализуемого приложения, относительно Bitcoin. Был сделан вывод, что базовые принципы умных контрактов были заложены уже в первом протоколе Bitcoin, однако они не были реализованы в клиентском программном обеспечении, и широко не использовались на практике. С появлением технологий, поверх протокола Bitcoin были созданы различные протоколы более высокого уровня, включая полноценные умные контракты, по аналогии с тем, как поверх TCP/IP существуют множество протоколов прикладного уровня.

В ходе анализа существующих аналогов был сделан вывод, что использование публичной сети для организации системы голосования предполагает значительные затраты на обеспечение безопасности. Данный вывод использован в так, что в дальнейшем при рассмотрении платформ для разработки блокчейн проектов будет сделан основной акцент на системах с частным блокчейном.

Во второй главе представлен анализ существующих платформ для разработки блокчейн систем, а также сравнение данных платформ. Основной акцент сделан на платформу Hyperledger Fabric.

Исследование основных платформ разработки блокчейн проектов показало, что Hyperledger Fabric наиболее применим для разработки смарт-контракта описывающего процесс голосования. В процессе сравнения другие аналоги показали себя либо как узкоспециализированые средства, либо как средства требующие работы с публичными блокчейнами, что в контексте решения поставленной задачи для корпоративных нужд недопустимо.

Обзор языка программирования Go, показал его широкие возможности и способы применения в процессе разработки чейнкодов. Была рассмотрена базовая структура чейнкода, так же были рассмотрены инструменты и программы доступные для разработки и сделан вывод, что Hyperledger предоставляет и поддерживает все необходимо для создания быстро работающих и надежных чейнкодов написанных на языке программирования Go.

Применяемые в настоящее время в работающих проектах схемы работы блокчейн приложений, показали, что Hyperledger созданы все условия для раздельной разработки блокчейн приложений. Сделанный выводы будут использованы в дальнейшей разработке приложения электронного голосования.

В третьей главе представлено проектирования программного средства, выбор алгоритма консенсуса, разработана схема сети. Также приведено описание разработки основных модулей программного средства и его тестирование на примере экспериментального использования в качестве средства принятия коллективного решения в корпоративной среде.

В ходе проектирования архитектуры программного средства голосования был рассмотрены модули необходимы для работы программного средства, которые работают все блокчейна, способы их создания и примененные технологии были использованы на основании исследований и анализа предыдущих глав.

Исследования возможных алгоритмов нахождения консенсуса в блокчейн сети Hyperledger Fabric показало, что все алгоритмы нахождения консенсуса призваны решать строго отведенные цели. В результате исследования было принято решение использовать стандартный алгоритм нахождения консенсуса, так как он позволяет организовать работу программного средства электронного голосования.

В ходе проектирования чейнкодов определяющих бизнес логику процесса голосования были построены схемы использованных алгоритмов и их описание. Были заложены возможности наделения голосующего пользователя не только лишь одним голосом, что является ключевой возможностью использования приложения в корпоративных средах с акционерным управлением.

На основе составленных схем алгоритмов было разработано и развернуто программное средство электронного голосования, произведено описание процесса его разработки. Основной упор сделан на описание реализуемых функций и их назначения.

Полученные в ходе тестирования данные свидетельствуют о том, что поставленные в данной работе цели и задачи были выполнены. Приведенный пример тестового использования подтвердил возможность использования программного средства для проведения электронных голосований.

ЗАКЛЮЧЕНИЕ

В процессе выполнения магистерской работы был произведен анализ уже существующих программных средств электронного голосования. В ходе анализа предметной области были обобщены достоинства и недостатки аналогичных решений, учтены при проектировании и разработке данного программного средства.

Были исследованы и сравнены современные блокчейн платформы. Были выявлены их достоинства и недостатки, также была выбрана платформа Hyperledger, как наиболее подходящая для создания программного средства электронного голосования.

Был рассмотрены технологии и алгоритмы разработки подобного рода приложений. Сделаны выводы о архитектуре позволяющей разработчику предоставить пользователям интерфейс для взаимодействия с блокчейном.

В результате проектирования программного средства электронного голосования были разработаны схемы алгоритмов работы отдельных модулей программного средства.

Как результат разработки архитектуры была представлена схема сети, в которой работает программное средство. На этапе создания программного средства была осуществлена разработка основного программного модуля, методов и функций в соответствии с составленной документацией.

В процессе разработки и интеграции написанных модулей производилось тестирование программного средства. На этапе тестирования были составлены тест кейсы для проверки работоспособности всех функций программного средства.

В результате выполненной работы, было получено работающее программное средство электронного голосования, позволяющее решить проблемы принятия коллективных решений в корпоративных средах. В дальнейшем данное программное обеспечение может быть улучшено расширенными возможностями настройки условий голосования, количества голосов у избирателей на основании некоторых показателей, например количества акций в организации, для которой проводится голосование.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых журналах

1. Анализ блокчейн технологий в контексте их использования для разработки прикладных программ / П.А. Богушевич // Интернетнаука. – 2020. – № 20(118).

2. Анализ информационных технологий, используемых в процессах голосования / П.А. Богушевич // Интернетнаука. – 2020. – № 21(119).