Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра математической теории упругости и биомеханики

Перспективы использования технологии blockchain в государственном учёте

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 441 группы

направления 09.03.03 Прикладная информатика

Механико-математический факультет

Андрушко Даниила Александровича

Научный руководитель
кандидат ю.н., доцент _____ Р.В. Амелин
подпись, дата

Зав. кафедрой
доктор ф.-м.н., профессор _____ Л.Ю. Коссович
подпись, дата

Саратов 2018

ВВЕДЕНИЕ

Внедрение технологии блокчейн как никогда актуальна в наше время. В 2016 г. международным аналитическим агентством Gartner был обнародован очередной прогноз до 2020 г., в котором представлены 10 трендов развития международной экономики и финансов. Все они, как отмечается аналитиками агентства, объединены общей темой происходящей цифровой революции, размах которой будет со временем расти. Среди топ-списка Gartner, впервые были обозначены блокчейн-технологии, как новое явление, способное изменить глобальную экономику и финансы.

Аналитики Gartner прогнозируют, что к 2020 г. оборот бизнеса, основанного на блокчейне, достигнет 10 млрд. долларов. Технологии распределенного реестра еще далеки от зрелости, но у них есть большой потенциал с точки зрения возможности экономии затрат в сфере финансовых и государственных услуг. Блокчейн можно использовать в любой отрасли, где требуется верифицировать транзакции.

Блокчейн – одна из самых перспективных технологических отраслей (наряду с Big Data, Machine learning, искусственным интеллектом), сравнимая по масштабу, степени влияния и распространению в будущем с тем эффектом, который в 1990-2000-е годы произвел интернет. По оценкам Всемирного банка, к концу 2018-го года уже 10% мирового ВВП будет храниться в блокчейне. Снижение издержек, повышение уровня безопасности и более высокая прозрачность транзакций – три главных сильных стороны блокчейна.

Наиболее перспективным использование блокчейн представляется в сфере автоматизации административных процедур с государственным участием, суть которых заключается во внесении юридически-значимых записей в те или иные реестры или регистры, отражающие гражданское состояние, права собственности, подтверждающие правоспособность или репутацию различных субъектов. Рост популярности блокчейна обусловлен в противовес стремлению государств к тотальному контролю и управлению. В первую очередь, это стремление людей и бизнеса защитить свою свободу и снизить издержки. В перспективе децентрализация придет и в государственное управление, его различные сферы учета, включая государственный, постепенно вытесняя централизованные модели. Важным аспектом по применению технологии блокчейн в государственном учете Российской Федерации является необходимость адаптации результатов мирового опыта к условиям отечественной экономики.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Целью бакалаврской работы является применение алгоритма технологии блокчейн в государственном учете в современных условиях перехода к «Цифровой экономике».

Для достижения цели бакалаврской работы необходимо решить следующие поставленные задачи:

- рассмотреть принцип работы технологии блокчейн

- определить сферы применения технологии блокчейн

- проанализировать типы блокчейна

- обосновать перспективы применения технологии блокчейн в государственном учете

Объектом исследования бакалаврской работы является государственный учет.

Предметом бакалаврской работы является сфера государственного учета в избирательном процессе.

Теоретические описание технологии блокчейн

Внимание к блокчейну привлекла возросшая популярность основанных на нем криптовалют. В 2009 году Сатоси Накамото опубликовал код биткоина, и криптовалюта торговалась по курсу 0,003 доллара за 1000 единиц – на текущий момент (31.05.2018 г.) она выросла в несколько сотен тысяч раз, превысив отметку в 7310 долларов за 1 единицу. Однако понятие и сферы применения блокчейна гораздо шире криптовалют. Особенности технологии распределенного реестра позволяют использовать его в большом числе отраслей – от коммерческих финансовых структур до защиты авторских прав и государственном учете подсчета голосов избирателей.

Основные понятия и алгоритм работы технологии блокчейн

Блокчейн – это выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащая информацию о транзакциях, защищенная криптографическим шифром и реализованная на основе децентрализованной базы данных. В начале технология блокчейн появилась в качестве инструмента для проведения транзакций с электронной валютой «биткоин». Уже сейчас блокчейн получил развитие как обособленная технология, которая может использоваться за рамками криптовалют. В России она получила название технологии распределенного реестра (англ.: Distributed ledger technology – DLT). Основным элементом блокчейна является журнал транзакций, при этом проведение транзакций – это единственный способ

изменить состояние реестра. Чтобы транзакция считалась состоявшейся и подтвержденной (необходимо согласие больше половины участников сети), ее формат и подписи должны быть проверены, и в случае валидации она (или группа транзакций) записывается в блок. Блок включает в себя список транзакций и заголовок (header), который содержит собственный хеш, хеш предыдущего блока, хеш транзакций и дополнительную информацию. Связь между блоками за счет наличия в каждом (за исключением первого) хеша предыдущего означает, что невозможно внести изменения в блок, не изменив всю цепочку с первого блока - нельзя удалить какую-то транзакцию или вставить ее между уже совершенных.

Любая транзакция в реестре признается действительной, только если ее одобряет более чем половины участников сети, то есть ни один участник системы или агент извне не могут провести валидную транзакцию без согласия других пользователей. Любая транзакция по своей сути – передача прав собственности. Природа такой операции подразумевает отсутствие взаимного доверия между участниками транзакции, для чего необходимо присутствие в сделке третьей стороны, которая бы гарантировала ее исполнение. Концепция блокчейна позволяет участникам системы достигать договоренностей о транзакции без участия и подтверждения со стороны посредника.

Исследователь и основатель института блокчейн-исследований (Institute for Blockchain Studies), М. Свон, выделяет три условные области применения данной технологии:

- Blockchain 1.0 - это валюта (криптовалюты применяются в различных приложениях, имеющих отношение к финансовым транзакциям, например, системы переводов и цифровых платежей);

- Blockchain 2.0 - это контракты (приложения в области экономики, рынков и финансов, работающие с различными типами инструментов - акциями, облигациями, фьючерсами, закладными, правовыми титулами, активами и контрактами);

- Blockchain 3.0 - приложения, область которых выходит за рамки финансовых транзакций и рынков (распространяются на сферы государственного управления, здравоохранения, науки, образования и др.).

Сферы применения технологии блокчейн

Для успешного внедрения в России технологии блокчейн в сфере государственного управления, рассмотрим уже имеющийся иностранный опыт ее применения. В начале 2016 г. в Великобритании был опубликован отчет «Технология распределенных реестров: за рамками блокчейн», представляющий исследование, проведенное Государственным управлением науки. В отчете, отмечается, что главная задача государства заключается в разработке четкой

концепции того, как обновленная технология распределенных реестров может улучшить взаимодействие государственных органов и каким образом она может быть использована для оказания услуг всем гражданам.

В настоящее время, прогресс обусловлен успехами реализации государственной программы «Информационное общество (2011-2020 гг.)», а также, итогами выполнения федеральной целевой программы «Электронная Россия (2002–2010 гг.)». Однако сфера информационных технологий является довольно динамичной в своем развитии и все чаще предлагает новые технологические решения в различных отраслях человеческой жизнедеятельности. К таковым относится инновационная технология распределенных реестров данных блокчейна. Появление и дальнейшее развитие этой новой технологии вызывает большой интерес как в научном, так и в бизнес сообществе. Технически блокчейн-решение может использоваться для осуществления любых соглашений, исключая при этом посредников, обеспечивая основу децентрализованным формам управления и социальным контрактам, основанным на консенсусе, позволяя поддерживать баланс в интересах общества.

Департамент информационных технологий Москвы выступил с предложением о реализации пилотного проекта по внедрению технологии блокчейна в качестве платформы системы электронных референдумов по портале «Активный гражданин». Помимо электронных голосований, есть и другие потенциальные применения блокчейна в госуправлении. На площадке уже зарегистрировано около 2 миллионов пользователей. За это время на платформе было проведено более 2,5 тысяч голосований. Эта платформа для проведения общественно значимых голосований, которая предлагает обсуждать самые разные вопросы, касающиеся жизни столицы. Здесь проводятся как общегородские, так и локальные голосования. Причем их участники могут не только повлиять на исход того или иного решения, но и получают за активность приятные бонусы. За каждую высказанную позицию пользователям начисляются баллы. Участники, кто набирает 1 тысячу баллов, могут обменять их на полезные сувениры или разнообразные услуги. Вдобавок также получают звание «Активный гражданин». Баллы начисляются еще за приглашение на площадку друзей и регулярное посещение сайта. Можно также повышать свой счет, делясь ссылкой на результаты голосований в соцсетях. В среднем на площадке появляется 1-2 новых опроса в неделю.

В ноябре 2017 года на портале для общественного обсуждения законодательных инициатив был опубликован проект плана мероприятий программы «Цифровая экономика Российской Федерации» по реформированию нормативно-правового регулирования. 18 декабря 2017 года план утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. Первая цель плана заключается в устранении ключевых правовых

ограничений и создании отдельных правовых институтов, направленных на решение первоочередных задач формирования цифровой экономики. Вторая – это создание постоянно действующего механизма управления изменениями и компетенциями в области регулирования цифровой экономики. Каждая цель включает ряд задач. В рамках регулирования правовых вопросов требуется сформировать условия для единой цифровой среды доверия и сферы электронного гражданского оборота, обеспечить внедрение и использование инновационных технологий на финансовом рынке и государственном учете, усовершенствовать механизмы стандартизации и прочее.

Блокчейн в государственном учете

Новые информационные технологии все чаще находят свое применение в жизни современного общества, затрагивая практически все его уровни. Не является исключением и сфера государственного управления. Более того, по мнению многих экспертов в последние несколько лет наблюдается существенный прогресс в использовании электронных каналов предоставления государственных услуг.

Основная проблема осуществления контроля заключается в человеческом факторе. При невозможности подделки голосов под пристальным взором наблюдателей данная операция вполне может быть перенесена в другое помещение. Отсутствие самой возможности полного контроля стирает грань доверия между избирателями и организатором выборов. Пассивность граждан – во многом следствие полнейшего разочарования в актуальной системе выборов. Распространено мнение, согласно которому поход на выборы не изменит ничего.

В вопросе легитимности блокчейна является настоящее решение, благодаря которому все насущные проблемы смогут быть устранены. Главное достоинство применения технологии – в возможности создания максимальной прозрачности выборов.

Технология блокчейн продолжает активно исследоваться и применяться по всему миру. Большие перспективы от её внедрения и использования видят и специалисты, и организации в самых разных сферах деятельности: от финансового сектора до институтов государственного управления. Одно из перспективных направлений применения этой технологии – это разработка на её основе прозрачных систем электронного голосования и учёта принимаемых решений. Существуют проекты, которые уже базируются на блокчейне, и они действительно являются альтернативой устаревшей системе. Создатели проектов утверждают: процесс прозрачен и подвергается проверке, все голоса уникальны. Еще одна площадка для проведения онлайн голосований, теперь международного образца – Follow My Vote. Платформа может применяться для проведения самых разных видов голосований, в том числе политических.

Система применима не только для политических, но и для многих других голосований. Используется одноранговая архитектура, что исключает возможность атаки DoS, здесь не имеется никакого центрального сервера. Однако, угрозу может представлять внедрение вредоносного программного обеспечения. Эта концепция проекта пытается вернуть прозрачность избирательной системе. Предлагается голосовать онлайн, идентификация через документы и веб-камеру. Каждый проголосовавший получает ID избирателя, по нему можно открыть избирательную урну, найти свой голос и перепроверить его. Также можно наблюдать за ходом голосования в реальном времени. Есть возможность менять свой голос до завершения дня выборов. Данная платформа достаточно удобна, что улучшит явку избирателей среди молодых поколений и предоставит более гибкие возможности живущим за границей, пожилым людям и инвалидам, даст альтернативу действующим методам голосования. Еще одно преимущество системы Follow My Vote – экономическая эффективность. Миллионы долларов налогоплательщиков расходуются на такие позиции, как печать бюллетеней и отправка по информации по разным каналам связи. Это ненужные затраты, которые со временем будут уменьшаться путем перемещения в онлайн. Все транзакции, которые происходят на блокчейне, проверяются независимыми нодами и подписывается криптографическим методом для обеспечения безопасности и анонимности. Система Follow My Vote дополнительно улучшает безопасность с помощью криптографии с использованием эллиптической кривой. Криптография обеспечивает безопасность и конфиденциальность, в то время как публичный леджер (книга всех записей) дает прозрачность и подотчетность.

В России «Национальный расчетный депозитарий» (НРД), центральный депозитарий России, завершил разработку и успешно протестировал прототип системы электронного голосования e-proxy voting на основе технологии распределенных реестров (блокчейн). Прототип разработан на базе сетевой распределенной криптографической платформы NXT, для обмена сообщениями использует международный стандарт ISO 20022. Разработка велась совместно с компанией DSX Technologies. Ее результаты доступны в виде открытого исходного кода (open-source) на GitHub. E-proxy voting представляет собой передовую технологию проведения корпоративных действий, при которой обмен информацией и документами. В НРД e-proxy voting впервые был внедрен в августе 2014 г., а в апреле 2015 г. технология была оптимизирована и приведена в соответствие с международными стандартами ISO. В апреле 2016 г. был протестирован прототип e-proxy voting на основе.

Существующая технология электронного голосования подразумевает обмен сообщениями каскадом через цепочки номинальных держателей от эмитента до владельца и в обратном направлении. НРД в этой цепочке ведет реестр голосования, обеспечивая передачу и подсчет инструкций по

голосованию. Прототип e-proxy voting на основе блокчейна регистрирует инструкции сразу в распределенном реестре, который поддерживают одновременно все участники цепочки. Распределенный реестр электронного голосования содержит полную историю обновлений, защищенную от искажений криптографическим шифрованием. При этом копии реестра хранятся у всех участников сети (номинальные держатели, НРД), и регулятору или аудитору достаточно просто присоединиться к данной сети, чтобы получить полный доступ ко всей необходимой для проверок информации. Данные, записанные в блокчейне один раз, не могут быть фальсифицированы – любые изменения процедуры или результатов голосования в распределенном реестре записываются, их копии распространяются среди всех участников сети и легко могут быть проверены, подчеркнули разработчики.

В «Национальном расчетном депозитарии», гражданин голосует в личном веб-кабинете на портале номинального держателя с использованием электронной подписи. Номинальный держатель записывает голос владельца в блокчейне, дополнив своей электронной подписью. В качестве подтверждения приема голоса номинальный держатель предоставляет владельцу идентификатор его голоса в распределенном реестре. Далее запись о голосе данного владельца последовательно подписывается номинальными держателями по цепочке до центрального депозитария. В момент завершения голосования система автоматически подсчитывает результаты, и НРД публикует их в блокчейне с использованием своей электронной подписи. При этом использование криптографических механизмов позволяет защитить промежуточные результаты голосования. Очень часто технология блокчейн находит свое применение при проведении всевозможных голосований.

В нашей стране в последнее время стали уделять большое внимание применению блокчейн технологий в государственных сферах. Центральный банк России с рядом крупнейших коммерческих банков создал блокчейн-консорциум, в рамках которого запущен корпоративный блокчейн – мастерчейн. Создаются финтех-акселераторы, появились первые блокчейн-стартапы. Однако темпы развития блокчейн-индустрии в России сдерживаются целым рядом факторов, основным из которых остается отсутствие адекватного законодательного регулирования.

Конституция Российской Федерации и основные международные договоры в сфере прав человека, такие как Всеобщая декларация прав человека 1948 года, Международный пакт о гражданских и политических правах 1966 года, Конвенция о защите прав человека и основных свобод 1950 года, закрепили основные гарантии осуществления избирательных прав. В частности, речь идёт о таких фундаментальных принципах, как всеобщее избирательное право, равное избирательное право, прямое избирательное право, тайна голосования и гласность, открытость выборов. Государство в соответствии с указанными

принципами должно обеспечить реализацию избирательных прав граждан, создать условия для изъязвления их воли. Очевидно, что в этом контексте государство обладает широким набором полномочий по организации выборов, их техническому и материальному обеспечению.

Решение возникающих правовых проблем при внедрении технологии блокчейн в избирательный процесс позволит это новой технологии в будущем устроить настоящую революцию в этой государственной сфере деятельности. Более того, реализация данной технологии в целом может существенно повлиять на состояние дел в сфере прав человека во всем мире включая нашу страну.

Анализ технологии блокчейн в контексте государственного учета

Существует множество реализаций технологии блокчейн, на основе которых можно выполнить поставленные передо мной задачи. Рассмотрим блокчейн-платформы, которые базируются на разных типах блокчейна. Чтобы выбрать подходящую платформу, проанализировать каждую в частности.

Типы блокчейн и используемые платформы

Приватные блокчейны – это блокчейны в которых блоки создаются централизованно, и все права на проведение операций принадлежат одной организации. Агенты извне могут только следить за транзакциями, в то время как проводить аудит, управлять базами и т.д. могут только доверенные узлы. Принцип работы приватных блокчейнов в следующем. Операторы формируют блоки по очереди с фиксированными временными интервалами - порядок либо определен, либо перемешивается после окончания цикла. Если участник не успел сформировать блок за определенное время, то он пропускает круг. Таким образом, если участниками транзакций являются только операторы данного приватного блокчейна, можно построить надежный протокол создания блоков без необходимости использования proof-of-work.

В публичных блокчейнах любой пользователь может создать блок транзакций – достаточно пройти соответствующий механизм верификации (proof-of-work или proof-of-stake). Эффективность системы достигается за счет обновлений протокола, предотвращающих преступные изменения. За счет этого достигается ее децентрализация – нет необходимости в ядре, в главном контролирующем органе.

Рассмотрим наиболее известные в мире блокчейн-платформы, упрощающие жизнь стартапам.

Ethereum – это блокчейн-платформа с открытым исходным кодом. Предназначена для смарт-контрактов и предоставляет инструменты программирования для их создания. Представленная Виталиком Бутериным в

2013 году, эта платформа упрощает как разработку децентрализованных приложений следующего поколения (DApps), так и договорные соглашения в онлайне. Ethereum позволяет разработку и выпуск криптовалют и имеющих хождение цифровых токенов. Больше того, вы можете создать собственную DAO (демократическую автономную организацию), например, виртуальную организацию, где разнообразные проблемы решаются путем голосования ее членов. Алгоритм консенсуса Ethereum – гибрид PoW (proof-of-work, доказательство выполненной работы) и PoS (proof-of-stake, доказательство доли).

BigChainDB – это распределенный реестр с открытым исходным кодом. Создана она для хранения большого количества данных. Система позволяет разработчикам развертывать доказательства-концепий (proof-of-concepts) и приложения блокчейна. Эта база данных предоставляет децентрализованный контроль, малое время ожидания, устойчивость, мощный функционал запросов и высокую скорость обработки транзакций. Система не имеет собственной криптовалюты, но позволяет выпуск и передачу любых активов, токенов и криптовалют. BigChainDB поддерживает пользовательские цифровые активы и устанавливает права доступа на уровне транзакции. BigChainDB основана на федеративной модели консенсуса, федерации узлов с правом голоса.

EOS – это блокчейн-платформа, которая предлагает большой набор возможностей для бизнес-проектов для фандрайзинга. Данная платформа является новой и основана на алгоритме асинхронных смарт-контрактов. За счет параллельного проведения большого количества транзакций система может проводить до 100 тысяч сделок в секунду. Это рекорд для блокчейнов. Здесь применяется консенсус DPoS (делегированного доказательства владения), при котором верификацию транзакций проводят выбранные «свидетели». Это сокращает число звеньев в цепочке и увеличивает скорость транзакций.

Проанализировав многие варианты блокчейн-платформ, для реализации поставленной цели работы, мною была выбрана Skipchain платформа. На ее базе будет создан блокчейн, который будет, в дальнейшем, применен в избирательном процессе.

Алгоритм применения технологии блокчейн в избирательном процессе

Применение технологии блокчейн в избирательном процессе представляет собой смену формы голосования и подвергает серьёзному переосмыслению ряд важнейших принципов избирательного права: принцип тайного голосования, принцип всеобщего голосования. Прежде чем приступить к рассмотрению разработанному, мною предложению по совершенствованию системы голосования с использованием технологии блокчейн, назовем ее условно – «система Блокчейн Anchor». Что такое Анкор? Анкор (в переводе с англ. anchor значит «якорь», «привязка»).

Разработанное мною предложение по совершенствованию избирательного процесса учитывает многоуровневую архитектуру, которая основана на блокчейн технологии платформы Анкора, можно назвать «Таблицей результатов голосования», является распределенной базой данных учета на основе архитектуры Skipchain. Данные в нашей «Таблице результатов голосования» криптографически связаны с Биткоин блокчейн через уровень Котена (Cotena), который обеспечивает неизменность и децентрализацию данных.

Анкора состоит из четырех технологических уровней: «Таблица результатов голосования» блокчейн, Cotena, Биткоин блокчейн и Votapp. Эти уровни связываются друг с другом на различных этапах в течение избирательного процесса.

«Таблицей результатов голосования» – это сеть обеспечивающая неизменность записи всех данных в течение избирательного процесса. Являясь памятью и постоянным хранилищем данных всей системы. Это распределенная база данных учета. Уровень «Таблицы результатов голосования» основан на Skipchain архитектуре, которая обеспечивает консенсусный механизм с высокой пропускной способностью и эффективной проверкой транзакции. Skipchain включают программные клиенты эффективно перемещаются по произвольно длинным блокчейн временным шкалам вперед и назад, предоставляя доказательство законности транзакции без потребности в полном отчете блокчейн. Обратные указатели в Skipchain – криптографические хеши, в то время как прямые указатели – коллективные подписи группой свидетелей. Таким образом программное обеспечение может проверить блок, на который ссылаются, при помощи криптографически проверенных маркеров, которые представляют многочисленную группу смежных блоков. Конечный результат – то, что даже ресурс-клиенты, используя мобильные телефоны, могут получить от эффективные проверенные обновления, используя трудно закодированную начальную версию программного обеспечения в качестве доверительной привязки. Такие клиенты не должны постоянно отслеживать цепочку выпуска, как биткоин, полный узел которого конфиденциально обменивается данными и

независимо проверяет блоки связей с предыдущим элементом, находящихся в офлайне.

Каждый блок в Skipchain состоит из следующих элементов данных:

- Корневой хеш дерева Меркле, содержащего все транзакции в текущем блоке и представление текущего состояния всего Skipchain;

- Хеш текущего блока, который действует как уникальный идентификатор для данного блока;

- Связь с предыдущим элементом Хеша, указывающий на предыдущий блок;

- Список прямых связей с предыдущим элементом, указывающих на различные блоки в Skipchain для быстрой навигации в цепочке;

- Список узлов Cothority, ответственных за обработку блока.

Которити (Cothority) – это узлы, которые защищают «Таблицы результатов голосования» и подтверждают транзакции. Каждый узел в сети поддерживает копию всех транзакций и утверждает новые транзакции в блоки как часть консенсусного механизма сети. Узлы независимо контролируют друг друга, чтобы гарантировать, что запись данных системы остается неизменной. Cothority на нашей платформе состоит из ряда серверов свидетеля, которые коллективно подтверждают транзакции в «Таблице результатов голосования». Транзакции состоят из избирательных бюллетеней, конфигурационный файл и консенсусное доказательство. Из набора узлов свидетелей, один из них определяется как «узел Оракула».

«Сервер Оракула» – это выбранный случайным образом один из серверов свидетелей. Он добавляет конфигурационный файл в «Таблице результатов голосования», создает блоки из аутентифицируемых избирательных бюллетеней. Также, добавляет подтвержденные блоки к журналу и продвигает их к биткоин блокчейн.

Котена (Cotena) – список снимков состояния «Таблицы результатов голосования», создающихся периодически во времени. Копия каждого журнала обновлений сохраняется узлами Cothority в биткоин блокчейн. Биткоин блокчейн является цифровой, децентрализованной базой, которая ведет учет всех транзакций. Данные, хранившие на децентрализованном блокчейн, не поддаются изменениям, делая блокчейн защищенным источником данных.

Вотапп (Votapp) – это уровень Front-and (приложение с интерфейсом). Создаётся приложение, для удобного пользования избирателем «Таблицей результатов голосования». Первичные приложения, которые будут существовать в уровне Votapp, включают «Кабину для голосования», «Аудит выборов» и «Узел Истории».

Приложение «Кабины для голосования» позволяет авторизованным избирателям участвовать в выборах. Избиратель в состоянии сделать свой «честный» выбор в системе голосования, полагаясь на анонимность, где выбранные данные по кандидатам сначала шифруются, позже отправляются в «Таблицу результатов голосования».

Необходимо предусмотреть так называемый «Аудит» – это базовая функция проверки в избирательной технологии. Приложение обеспечивает доступный комплект инструментальных средств для контроля выборов в любом месте в течение избирательного процесса. Любой проголосовавший избиратель может выполнить запрос на «Узел Истории» в сети, где находится полная история «Таблицы результатов голосования» и журналы Cotena. «Узел Истории» может ответить на запрос любого клиента, чтобы запросить «Таблицу результатов голосования», но не в состоянии активно участвовать в сети, действуя как сервер свидетеля. Для этого узла, чтобы действовать в качестве сервера свидетеля, это должно быть оценено как партнерство в сети.

До начала администрирования выборов, администраторы начинают событие выборов, создавая конфигурационный файл, который включает специфичные для события параметры. Полный набор параметров включает:

- Список Выборов. Эти значения включают имена и открытые ключи (идентификаторы), сгенерированный через протокол распределенной генерации ключей (DKG).

- Выборы Запускаются/оканчиваются. Эти значения указывают период времени, в который голосующим избирателям разрешается проголосовать.

- Список Избирателей. Этот список содержит всех избирателей, имеющих право голосования на данных выборах. Согласно сценария, список может быть открыт, т.е. идентификационные данные избирателей, защищенные anonymization (обезличенными) методами, становятся известны.

- Список кандидатов и Выбор. Это список кандидатов и вопросов, отвечая на которые избиратели принимают свои решения самостоятельно.

- Список Аудиторов. Для некоторых выборов, могут назначаться официальные аудиторы (наблюдатели от политических и общественных организаций), ответственность которых включает проверку события выборов и посредничество спорах, которые могли бы произойти во время выборов. Если аудиторы указаны, их идентификаторы и связанные открытые ключи должны быть включены в систему выборов.

Как только параметры выборов вводятся в конфигурационный файл, администраторы генерируют уникальный криптографический идентификатор для конфигурационного файла через криптографическую хеш-функцию, которая может действовать как представление ID события выборов. Администраторы также подписывают конфигурационный файл с идентификатором, чтобы доказать, что они действительно организаторы события выборов. Далее,

подписанный и конфигурационный файл сохраняется в «Таблице результатов голосования» Анкоры.

Как только конфигурационный файл отправлен в «Таблицу результатов голосования», он становится доступным для всей общественности. Если конфигурационный файл одобрен общественностью и другими заинтересованными сторонами, система полностью работоспособна и честно выполняет свои функции перед избирателями выдавая итоговый результат голосования в реальном времени.

Как только фаза кастинга началась, каждый имеющий право голосовать избиратель может быстро проголосовать на выборах. Избиратель может получить доступ к своей «виртуальной» кабине для голосования через цифровое устройство голосования, которое позволяет заполнять, рассматривать, изолировать (шифровать) и подсчитывать итоги голосования.

Анкора позволяет избирателям участвовать при помощи любого персонального устройства, такого как смартфон или компьютер, или при помощи машины для подсчета голосов в традиционном избирательном центре.

Когда избиратель отдает голос, он зашифровывается программным обеспечением с коллективным открытым ключом Cothority, которые являются распределенными узлами свидетеля платформы Анкоры. Каждая избирательная система должна гарантировать конфиденциальность своих избирателей. Как только время голосования заканчивается, сеть Анкора работает так, что все избирательные бюллетени шифруются, чтобы анонимизировать зашифрованные избирательные бюллетени, которые поступают в «Таблицу результатов голосования».

Чтобы выполнить процесс соответствия, узлы Cothority коллективно дешифруют анонимизированные избирательные бюллетени и публикуют их с доказательствами правильности дешифрования в «Таблицах результатов голосования». Чтобы начать этот процесс, узлы Cothority проверяют что доказательства нулевого знания от фазы анонимизации корректна, и, если так, узлы начинают коллективно дешифровать анонимизированные избирательные бюллетени. В этом процессе каждый узел Cothority частично дешифрует каждый из анонимизированных голосов и генерирует нулевое доказательство знаний для каждого дешифрования, свидетельствуя о правильность частичного дешифрования. Далее, все узлы Cothority публикуют свои результаты в «Таблице результатов голосования». Администраторы выборов могут проверить что доказательства нулевого знания дешифрованных избирательных бюллетеней корректны.

После фазы дешифрования узлы Анкоры соответствуют голосам через все допустимые дешифрованные избирательные бюллетени и публикует конечные результаты в «Таблице результатов голосования». Сторона, официально ответственная за соответствие голосам, отправляет конечные результаты в

«Таблицу результатов голосования», в которой аудиторы (наблюдатели) имею право проверки законности результата, прежде чем это будет считаться окончательным. Когда принято последнее решение, Анкора проведет автоматизированный подсчет всех голосов. В то время как администратор выборов решает, какая сторона будет ответственна за официальный подсчет, любой может проверить свой поданный голос на данных выборах.

Способность контролировать результаты выборов на каждом этапе избирательного процесса является одним из главных преимуществ к применению платформы Анкоры. Официально назначенные аудиторы (наблюдатели) на данных выборах в итоге засвидетельствуют законность выборов, отправляя подписанное заявление в «Таблицу результатов голосования». Если избирательный процесс успешно проверен по словам официального аудитора, заключительной аттестации подписан с аудиторским закрытым ключом.

Многие попытки придумать эффективные схемы голосования, защищенного от основных видов фальсификаций, основываются на том или ином способе отказа от тайны голосования, игнорируя возникающие при этом опасности облегчения покупки голосов или принуждения избирателя к голосованию. Эти опасности, неизбежно вытекают из необходимости сочетать «несочетаемые» требования честных выборов – обеспечения возможности избирателю проверить, как учтен его голос, и исключения возможности продать свой голос – то есть доказать покупателю, как именно он проголосовал. Учет первого требования приводит к отказу от тайны голосования, и, автоматически, дает этому избирателю возможность продать свой голос тому, кто захочет его купить. Возможность продажи голоса автоматически означает появление возможности принуждения избирателя голосовать по требованию злоумышленника под угрозой преследования или дискриминации. Фактической покупки голосов или принуждения может и не быть – достаточно самой угрозы и возможности такой покупки для возникновения опасности дискредитации результатов голосования. Существующая в большинстве стран система голосования с анонимными избирательными бюллетенями появилась неслучайно. Этот вариант позволяет учитывать свободное волеизъявление граждан, не раскрывая их собственных предпочтений в выборе кандидата при голосовании на избирательном участке.

ЗАКЛЮЧЕНИЕ

Поставленные задачи в бакалаврской работе полностью выполнены. Подробно рассмотрены темы: технология блокчейн и основные его понятия, обозначены сферы применения технологии блокчейн, позиционированы перспективы применения блокчейна в государственном учете избирательной системы. Была достигнута цель работы, в которой подробно рассмотрен и применен алгоритм технологии блокчейн в государственном учете избирательного процесса.

Блокчейн дает результаты, превосходящие другие по обеспечению безопасности проведения голосования. За счет электронной подписи проводится идентификация пользователя. Новая технология позволяет разделять роли в системе голосования и учета (оператор, аудитор, рядовой пользователь) таким образом, чтобы не позволять всем участвовать, в подтверждении транзакций. У блокчейна высокий уровень криптографической защиты, поскольку блоки состоят из хеш-сумм, а по хеш сумме нельзя однозначно определить предмет транзакции и другие входные данные. Главное достоинство применения технологии – в возможности создания максимальной прозрачности выборов.

Открытость данных позволит в любой момент проверить достоверность поданного голоса каждого участника выборов. Высокая защищённость информации гарантия от взломов и фальсификации. У избирателей появляется возможность самостоятельно следить за ходом выборов в режиме реального времени, при это подсчет голосов будет происходить по мере ведения голосования.

Блокчейн-выборы невозможно фальсифицировать, а всю информацию о кандидатах можно узнать в несколько кликов и быть уверенным, что информация подлинная. Там, где все контролируется всеми, государственные институты будут выполнять лишь технические функции по обслуживанию децентрализованного сообщества. Решение возникающих правовых проблем при внедрении технологии блокчейна в избирательный процесс позволит этой технологии, как способу реализации волеизъявления избирателей устроить в будущем настоящую революцию в этой государственной сфере деятельности. Более того, реализация данной технологии в целом может существенно повлиять на состояние дел в сфере прав человека во всем мире включая нашу страну.