Горячкин Б.С.,
кандидат технических наук, доцент
доцент кафедры «Системы обработки информации и управления»
Московский государственный технический университет
Россия, г. Москва
Адамян П.С.,
студент 4 курс, факультет «Информатика и системы управления»
Московский государственный технический университет
Россия, г. Москва
Бритиков К.И.,
студент 4 курс, факультет «Информатика и системы управления»
Московский государственный технический университет
Россия, г. Москва

СИСТЕМЫ ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннотация: *В данной статье будут рассмотрены современные системы голосования на основе технологии блокчейн, а также технологии и методы, применяемые в их разработке.*

Ключевые слова: *блокчейн, БЭГ, голосование, биткоин, РСОД, VoteWatch, VoteBook, Proposal, IDecide, криптовалюта, голос.*

Annotation: *Modern blockchain election voting systems will be reviewed in current article, as well as the technologies and methods used for their development.*

Key Words: *blockchain, BEV, election, bitcoin, DDPS, VoteWatch, VoteBook, Proposal, IDecide, cryptocurrency, voting.*

Блокчейн – это недавно разработанный метод для распределенного хранения данных. Его суть состоит в распределенном хранении цепочки блоков, при этом данная цепочка полностью реплицируется на каждую машину в системе[1,6].

В прошлом году эта система пережила пик популярности, в связи с возникшим высоким интересом к криптовалютам, основанным на этой системе. Сейчас информационное освещение блокчейна заметно спало, но при этом к нему существует огромный интерес в сферах, не связанных с валютой. Одной из таких сфер является применение блокчейна для создания открытых и анонимных систем для голосования.

Блокчейн идеально подходит для создания безопасных систем, которые обеспечивают полную анонимность человека, отправляющего транзакцию, поэтому такую систему теоретически почти невозможно будет взломать и обмануть.

Блокчейн и голосование

Следуя Оксфордскому словарю английского, демократия – это система управления, при которой в управлении участвует все население, или представители населения, которые, как правило, определяются избирательным путем. Исходя из определения, для того, чтобы демократия работала, необходимо производить голосование. Голосование – это базис любого демократического государства, и оно должно быть доступным и безопасным для всех граждан. Существующие сегодня избирательные системы дешевы и доступны, но у них есть две основные проблемы. Во-первых, они плохо масштабируемы, а во-вторых, они полагаются на безопасность процедур, при которых сотрудники ЦИК должны исполнять свою работу правильно и честно. Дополнительно к этому существующие системы взаимодействуют с электронными системами голосования, что порождает целый набор уязвимостей [3,с. 8]. В связи с этим современные выборы могут быть сфальсифицированы под влиянием правительства или какой либо партии. Аналогичные проблемы распространяются на все системы голосования, вне зависимости от того, государственные они, или нет. Блокчейн может помочь решить эту проблему.

Электронное голосование – это ключевой общественный сектор который может быть радикально изменен технологией блокчейн. Идея блокчейн электронного голосования (БЭГ) крайне проста. БЭГ, аналогично

криптовалютам, назначает каждому избирателю «кошелек», содержащий данные пользователя. Каждый избиратель получает единственную «монетку», которая позволяет отдать свой голос один раз. Однако голосующие могут изменить свой выбор перед окончанием голосования.

Избиратели могут анонимно проголосовать, используя компьютер или телефон. БЭГ обеспечивает пользователей зашифрованным ключом и секретным личным идентификатором. Например, мобильная система электронного голосования из Бостона «Voatz» использует умную биометрику для верификации идентификатора в реальном времени. Публичность и распределенность системы обеспечивает то, что каждый голос будет привязан к определенному избирателю и обеспечит постоянную неизменяемую запись голосования[2].

Еще одним вариантом решения проблемы идентификации личности в подобных системах является централизованное управление. Например, государство обеспечивает доступ человека к системе, основываясь на предоставленных документах.

Существующие системы БЭГ тестировались на информационных и консультативных голосованиях. К примеру ранее упомянутая Voatz[7] использовалась для выборов в студсовет, голосований в церковных организациях и местных мероприятий политических партий. Данная система также используется в городском совете Массачусетса.

Другая такая система была запущена в феврале 2018 в Москве, для муниципальной программы «Активный гражданин». Чтобы проверить безопасность БЭГ, мэрия заказала аудит у компании PwC, в результате аудита не было найдено ни одной уязвимости в системе для голосований, в которых приняли участие более 300000 человек.[4]

Уязвимости блокчейн

Несмотря на очевидные преимущества, у блокчейна есть две большие, и практически неразрешимые уязвимости. Это уязвимость к атаке 51% и проблеме двойной траты.

Проблема 51% состоит в том, что блокчейн считает истинной ту цепочку, которую считает истинной более половины системы, то есть если злоумышленники будут владеть более чем 51% вычислительных мощностей системы, то по сути они смогут ей управлять и изменять так, как им пожелается. Уязвимость к атаке 51% – это своего рода болезнь блокчейн систем, причем болезнь смертельная. Но при большом количестве участников в системе проведение такой атаки практически невозможно, потому что злоумышленники не смогут заполучить подобные вычислительные мощности в системе, ограниченной по количеству избирателей и токенов.

Двойная трата – это когда злоумышленник одновременно отправляет транзакцию к двум участникам системы (в случае выборов два варианта голосования). Но данная атака также требует огромных вычислительных мощностей. Например для покупки в магазине при помощи криптовалютной системы Bitcoin, если у атакующего находится 10% вычислительной мощности (hashrate) сети Bitcoin, а магазин, для успешного проведения транзакции, ждет 6 подтверждений — вероятность успеха такой атаки составит 0.1%.

Из описанного выше видно, что несмотря на существование уязвимостей системы, ее взлом сложен, а для больших голосований областного и государственного уровня практически невозможен.

Существующие платформы голосования на основе технологии блокчейн

Системы БЭГ начали активно проектировать с 2016 года, и на сегодняшний день существуют уже несколько готовых систем. Рассмотрим самые известные из них.[8]

VoteWatch

VoteWatch разработан американской компанией Blockchain Technologies Corp. в качестве подсистемы для бумажного голосования. Это проект с открытым исходным кодом, что обеспечивает значительную прозрачность, важную для подобных систем. Данная система предназначена для компаний, правительства, трудовых объединений.

Разработанная ими технология закрепляет каждому бюллетеню QR-код, что предотвращает его использование дважды. Данные токены также служат для разблокирования единичного голоса, который поступает кандидату при помощи блокчейна.

Информация о выборах загружается в две публичные цепочки блоков, Биткоин и Флоринкоин. В результате выборов две этих цепочки соединяются и сверяются, показывая результат голосования.

Данная система обеспечивает удобный аудит безопасности голосования, она поддерживает несколько методов для проведения полного аудита. Бумажные записи могут быть сверены с электронными результатами, которые невозможно изменить или переписать, так как они записываются на DVD с одноразовой записью.[2]

VoteBook

Несмотря на плюсы оригинальной блокчейн сети Биткойна, мы не можем использовать ее для проведения электронных голосований. Такая система должна отвечать следующим правилам:

1. У избирателя должна быть возможность убедиться, что его голос был учтен. Однако информация о выборе должна быть скрыта от остальных участников
2. Необходима возможность подведения промежуточных итогов
3. У избирателей должно быть право воздержаться, тогда их голос не должен учитываться
4. Если результаты выбора будут оспорены, то система должна подлежать аудиту

В данном проекте исключена возможность проведения удаленного голосования: во-первых далеко не у каждого есть компьютер с доступом к интернету, во-вторых, даже если всем дать такую возможность, то это влечет за собой множество уязвимостей. Проверка личности избирателя – весьма трудоемкий процесс. В доме избирателя может быть третья принуждающая сторона. К тому же злоумышленник с минимальными ресурсами может предпринять DoS атаку (denial of service) в пределах района. Исходя из всего

вышеперечисленного, авторы данной системы пришли к выводу, что самым безопасным вариантом будет комбинация традиционного подхода голосования (бумажные бюллетени) на этапе внесения голоса с блокчейн технологиями на этапе учета голоса и подведения итогов.

Проект VoteBook заимствует большинство идей у Биткойна, однако с некоторыми дополнениями. Как и в Биткойне, здесь используется распределенная база данных, где ретроактивные изменения отсутствуют, а для внесения изменений должно быть специальное соглашение. Здесь, в отличие от Биткойна, не применяется механизм доказательства проделанной работы (PoW - proof of work). Данный подход применяется в системах для ограничения прав, где нету доверия среди участников, однако это не так, когда речь заходит о проведении выборов. Для этого авторы системы предлагают ввести некий центральный орган, который будет распределять ключи шифрования среди узлов. Таким образом мы приходим к permissioned блокчейну.

Proposal

Рассмотренные ранее системы были централизованными, Proposal был разработан для того, чтобы решить эту проблему. Это проект с открытым исходным кодом, который создается независимыми разработчиками.

Об этой системе нет подробной информации в сети, поскольку она все еще находится в процессе разработки, но по заверениям создателей эта система, в отличие от предыдущих, позволит осуществлять удаленное голосование, более того, она будет распределенной и масштабируемой, то есть у нее не будет какого-то уполномоченного узла, который будет иметь повышенные права.

В то же время система обеспечит привязанность голоса к избирателю, а следовательно не допустит махинаций в процессе. Пока что это одна из наиболее перспективных систем, которые разрабатываются при помощи технологии блокчейн.[3]

iDecide

Это проект, разработанный командой отечественных программистов. У них описана самая открытая документация. Ниже приводится детальное

описание системы от самих разработчиков. Структурная схема голосования выглядит следующим образом:

Структура системы разделена на 3 сегмента:

UI – приложения конечного пользователя, которые подключаются к общедоступным REST API (Common Area сегмент) или непосредственно к читающему узлу БЧ (на схеме не отображен). В прототипе для демонстрации функционала мы реализовали UI веб сайт как SPA на Angular. Любой желающий может реализовать свой UI на любой доступной технологии, используя наши REST API или Read only узел Multichain в качестве источника данных.

Common Area – это N узлов системы, на которых развернут Multichain в режиме записи и Web сервер с API для общего доступа.

REST API веб сайт, написанный на ASP.NET Core 1.1. Реализована работа с метаданными голосования, архивом метаданных, самим процессом голосования (выбор варианта и отдача голоса за него), а также кошельком пользователя.

Private Area – закрытая для общего доступа (записи) часть системы, в состав которой входит процессинговый сервер и сервер авторизации пользователей.

Не смотря на очевидные достоинства данный проект не был закончен, и так и остался в фазе тестирования. К тому же данный проект не защищал от возможности пользователя проголосовать несколько раз, поскольку не привязывал определенного пользователя к ключам.[5]

Существующие на данный момент системы голосования, на основе технологии блокчейн как правило обладают каким-либо централизованным узлом, а следовательно не являются РСОД в прямом ее понимании. На данный момент создание распределенных независимых систем голосования только начинается, поскольку еще не существует системы, удовлетворяющей всем требованиям безопасности и удобства.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Satoshi Nacamoto.–статья о биткоине от его создателя. // Bitcoin: A Peer - to - Peer Electronic Cash System. Электронный ресурс // https://bitcoin.org/bitcoin.pdf
2. VoteWatcher -- официальная страница БЭВ. Электронный ресурс // http://votewatcher.com/
3. Докуметация БЭВ VoteBook. Электронный ресурс // https://www.economist.com/sites/default/files/nyu.pdf
4. Статья о разработке БЭВ.//Как создать систему электронного голосования на блокчейне. Электронный ресурс // https://habr.com/post/340342/
5. IDecide -- официальная страница БЭВ. Электронный ресурс// https://ui.demo.idecide.io/dashboard.
6. Pedro Franco.The Blockchain// Understanding Bitcoin: Cryptography, Engineering and Economics.—John Wiley & Sons, 2014.—288 p.— ISBN 978 - 1 -119 - 01916 – 9
7. Voatz – официальная страница БЭВ, с кратким техническим описанием. Электронный ресурс// https://voatz.com/
8. Хранилище электронной документации о технологии блокчейн, ее уязвимостях и разновидностях. Электронный ресурс// https://ru.bitcoinwiki.org/wiki