УДК 004.056.2

ПРИМЕНЕНИЕ БЛОКЧЕЙН-СИСТЕМЫ В СФЕРЕ ПРОВЕДЕНИЯ ГОЛОСОВАНИЙ

Бекк А.Е., студент гр. ИТб-172, IV курс
Кислицина А.С., студент гр. ИТб-172, IV курс
Сыркин И.С., к.т.н. доцент кафедры ИиАПС
Асанов С.А., старший преподаватель кафедры ИиАПС
Кузбасский государственный технический университет имени Т.Ф. Горбачёва
г. Кемерово

С каждым днем сфера онлайн-услуг развивается всё стремительнее, упрощая многие аспекты социальной жизни граждан. В области работы органов государственного управления также наблюдается тенденция перехода на удаленную работу с населением (приём и обработка обращений, подача документов для получения государственных услуг и прочее). Однако такие масштабные мероприятия, как федеральные и региональные голосования, при дистанционном проведении требуют особой подготовки для обеспечения безопасности персональных данных граждан без нарушения тайны голосования.

Растущие вычислительные мощности персональных и мобильных устройств способствуют развитию клиентских приложений, которые всё меньше и меньше ограничены ресурсами устройств, поэтому с каждым годом технология блокчейн становится всё актуальнее, так как главный её минус – требование к постоянному наличию вычислительного ресурса на устройстве с узлом, – постепенно становится всё менее актуальным.

Данная статья посвящена разработке блокчейн-системы удаленного голосования. Подразумевается, что валидность и уникальность пользователей будет подтверждаться авторизацией на портале госуслуг, возможны варианты с содержанием узлов как исключительно на государственных ресурсах, так и на устройствах заинтересованных граждан.

Что же такое блокчейн-система? Это децентрализованное хранилище криптографически защищенных транзакций, формирующих цепочку блоков. Структура представляет из себя цепочку блоков, также являющуюся связным списком, но определенного формата (Рис. 1).

Каждый блок представляет из себя перечень транзакций, которые записаны в этот блок, уникальный номер блока, работающий в роли криптографической соли, а также хэш заголовка предыдущего блока. Здесь виден первый принцип, обеспечивающий безопасность данных в блокчейне – хэши предыдущего блока хранятся в новом блоке, поэтому, если злоумышленник изменил данные в каком-то блоке, то простое сравнение хэша данного блока и хэша этого же блока, хранимого в следующем блоке, позволит однозначно установить недостоверность данных.

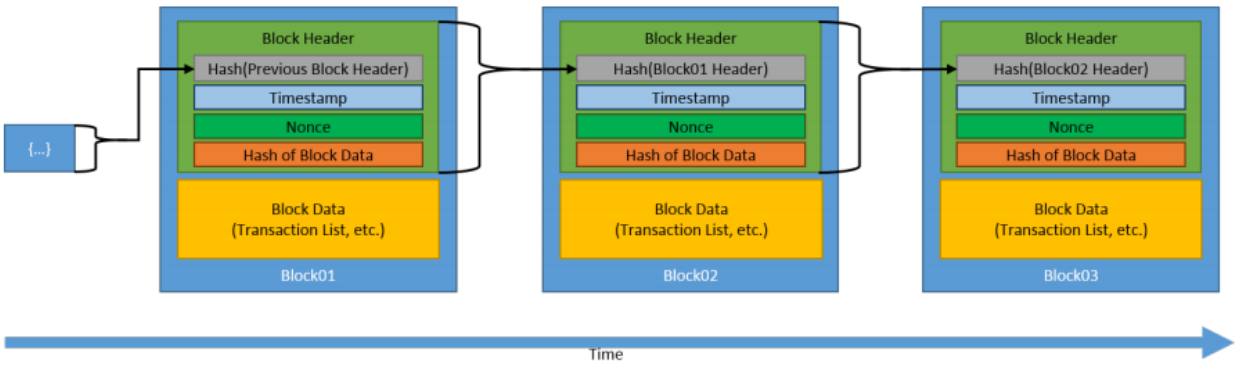

Рис 1. Схема представления формата блокчейна

В нашем случае транзакция будет представлена в виде:

- результатов заполнения электронного бюллетеня в открытом незакодированном виде;
- публичного ключа пользователя.

Таким образом анализ списка транзакций позволит без затруднений подсчитать голоса, при этом не разглашая персональных данных пользователя, а публичный ключ позволит самим гражданам однозначно убедиться в том, что их голос учтен.

Авторизация на госуслугах разрешает проблему проверки документов граждан, а также создания уникального ключа пользователя, как приватного, хранимого пользователем, так и публичного, который будет записан в блокчейне. Удобнее всего представляется приватный ключ из последовательности ФИО, серии и номера паспорта с любыми разделительными символами, либо с использованием электронно-цифровой подписи при её наличии. Публичный ключ удобно представить в формате результата одностороннего шифрования приватного.

После определения безопасной структуры данных, остается определить алгоритмы, которые позволят децентрализировать хранение этих данных по различным устройствам любых пользователей, добавляя ещё один слой безопасности. Первым эти алгоритмы строго определил Сатоши Накамото в своей статье «Bitcoin: A Peer to Peer Electronic Cash System» от 2008-го года, в которой описывается система криптографической валюты на базе блокчейна, с широко применяемым методом консенсуса.

Одним из ключевых пунктов работы децентрализованной блокчейн-системы является определение того, какой пользователь следующим опубликует новый блок, т.к. чаще всего в рамках блокчейна существует множество узлов, которые готовы опубликовать новый блок в одно время, причем, возвращаясь к блокчейнам с наградой в виде криптографической валюты, любой узел не заинтересован в том, чтобы кто-либо другой сделал публикацию блока первым, поэтому надо определить точки согласия для всех пользователей, который неоспоримы. Данными точками согласия являются:

- первичный блок системы, исходное состояние системы;
- общепринятый метод консенсуса;

- правила связывания блоков;
- возможность проверки цепочки блоков любым пользователем.

На практике данные пункты соблюдаются при помощи ПО без необходимости участия пользователя.

Рассмотрим самые популярные методы консенсуса, разрешающие проблему публикации следующего блока среди узлов (здесь пользователи):

- Proof of Work (доказательство проделанной работы, англ.) – механика, по которой право публикации отдается первому пользователю, который решит некоторое сложное вычисление и обменяется данным решением. В данном случае публикует первый пользователь с наибольшей вычислительной мощностью устройства, остальные пользователи публикуют блоки следом по порядку скорости вычисления, без повторных вычислений для следующих блоков;
- Proof of Stake (доказательство ставки) в данной модели первым публикуется блок пользователя, который имеет наибольше количество уже опубликованных блоков, транзакций или других записей, подтверждающих его активное взаимодействие с системой;
- Round Robin (круговая система) выстраивается случайный порядок из пользователей, который формируется с целью равномерного распределения публикуемых блоков среди пользователей;
- Proof of Authority/Proof of Identity (доказательство авторитета) каждый пользователь находится в некоторой иерархии реального мира, которая определяет порядок публикации блоков. Например, директор компании вносит свой блок быстрее остальных работников;
- Proof of Elapsed Time Consensus Model (доказательство прошедшего времени) ПО пользователя генерирует случайную временную задержку перед отправкой нового блока, тем самым образуя случайный порядок из пользователей.

Предпочитаемая модель консенсуса блокчейна зависит от назначения блокчейн-системы, т.к. в конечном счете она только лишь определяет взаимодействие узлов децентрализованного сервера. Для нашей предполагаемой системы рациональнее всего использовать доказательство прошедшего времени, т.к. порядок голосования не играет никакой роли и не приносит никакой выгоды узлам.

Каждый узел блокчейн-системы может являться равноправным сервером и клиентом одновременно, как в классической P2P-сети (Рис. 2). Это приводит к хранению самого блокчейна на неопределенном количестве устройств, каждое из которых не только публикует новые блоки, но и проверяет новые опубликованные блоки, что обеспечивает ещё одну ступень защиты для хранимых транзакций. Если злоумышленник взломал одно устройство из данной сети, то остальные просто не примут замененные блоки из-за несоответствия блокчейнов на других устройствах. Вариант совмещения клиента и сервера применим в нашем случае для граждан-добровольцев, которые не против разместить на своих устройствах узлы для усиления уровня безопасности голосования.

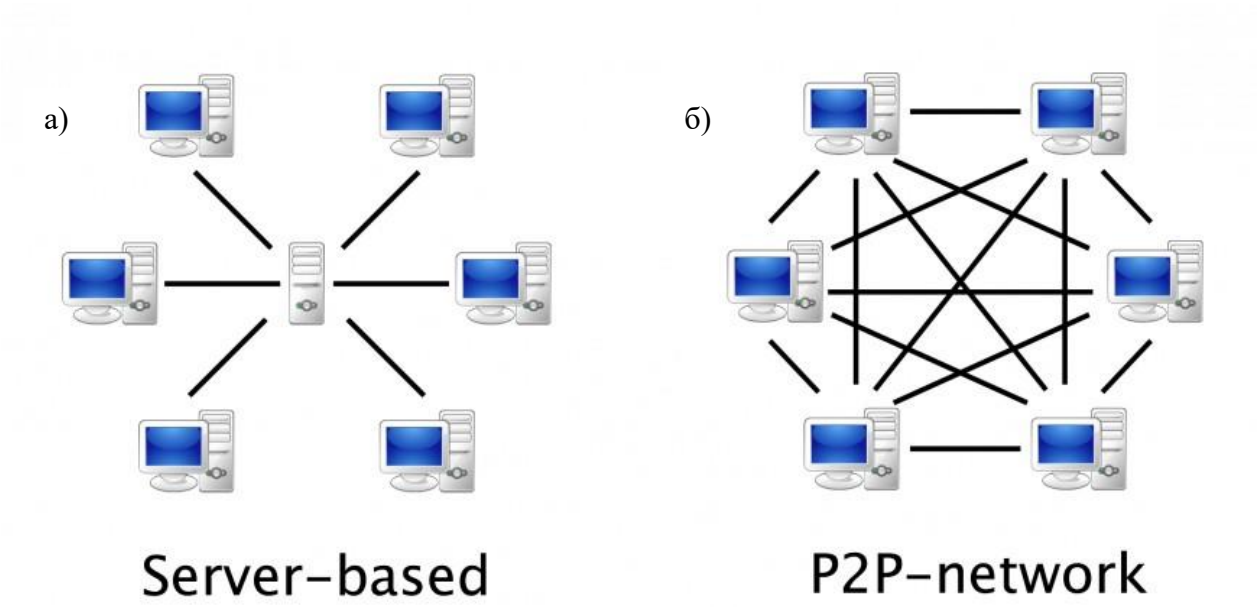

Рис 2. Схемы взаимодействия сети формата сервер-клиент (а) и P2P-сети (б)

В заключении стоит отметить, что исследуемая система позволяет перейти на качественно новый уровень безопасности, при этом позволяя гражданам голосовать удаленно, обеспечивая расширение функционала уже существующих ресурсов в области государственного управления.

Список литературы

1. D. Yaga, P. Mell, N. Roby, K. Scarfone. Blockchain Technology Overview. // Библиотека Национального Института Стандартов и Технологий [сайт]. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. // Информационный портал [сайт]. URL: https://bitcoin.org/bitcoin.pdf
3. Sourav Sen Gupta. BLOCKCHAIN:The foundation behind Bitcoin. Научная библиотека Индийского Института Статистики [сайт]. URL: https://www.isical.ac.in/~debrup/slides/Bitcoin.pdf