ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Курбатов А.С.
Научный руководитель – доцент кафедри БИТ, к.т.н. Петренко О.Е.
Харьковский национальный университет радиоэлектроники
(61166, Харків, просп. Науки,14, каф. Безопасности информационных технологий, тел.: т. 093-510-55-49)
email: olkurbatov@gmail.com

Traditional accounting systems require complete user trust. A centralized approach in building payment systems, property accounting registers, voting platforms has its advantages, but at the same time it forces the end user to blindly believe the final state of the accounting system database. Therefore, it is not surprising that the community was interested in the systems, which made it possible to guarantee the compliance of the accounting system's database with the conducted transactions, while trusting only the mathematical methods on which they are based. The blockchain technology has become the key to building such systems.

Целью данной работы является анализ технологии, которая применяется в децентрализованных системах голосования, и постановка задач, которые требуют решения перед внедрением таких систем.

Децентрализованная система электронного голосования – децентрализованная учетная система, в которой идентификаторы пользователей строго привязаны к их личностям, но все действия пользователей должны быть анонимны (связать личность и идентификатор пользователя можно, но связь идентификатора пользователя с действиями в учетной системы, не является возможной без явного желания пользователя). Все действия участников системы записываются в распределенную базу данных в виде отдельных транзакций. При подтверждении, транзакции объединяются в блоки образуя неизменяемую цепочку блоков, доступ к которой имеет любой желающий [1].

Как было определено выше, идентификаторы пользователей должны быть строго привязаны к их личностям. Единственный на сегодняшний день способ обеспечения этого требования – предварительное внедрение государством системы digital identity и предоставление сертификата открытого ключа каждому из голосующих. На сегодняшний день получение сертификата открытого ключа не является проблемой. Поэтому стоит рассматривать два подхода: одноразовая предвыборная сертификация (одноразовое получение ключей для возможности проголосовать) либо использование ранее полученных сертификатов. Оба подхода имеют свои преимущества, однако каждый из них также сопровождается рядом проблем.

Обеспечить тайну голосования достаточно просто. Для этого можно использовать механизм кольцевой подписи, позволяющий пользователю скрыть свой голос среди участников группы [2]. Важно отметить при этом, что каждый голос должен обладать свойством fungibility, то есть должен быть неотличимым от других голосов, иначе тайну голосования обеспечить будет невозможно. Поэтому структура транзакции должна быть строго определена и должна исключать возможность добавления каких-либо произвольных данных.

Теперь стоит рассмотреть кто может быть валидатором на платформе голосования. Потенциально роль валидатора может выполняться теми же комиссиями, которые на данный момент проводят голосование. Количество комиссий должно быть строго ограничено, валидаторы должны быть идентифицированы (и связаны с сформированными ими блоками).

Таким образом, можно сделать вывод, что децентрализованная система электронного голосования – система, которую вполне реально построить при использовании математических методов и алгоритмов достижения консенсуса. Однако, на сегодняшний день построение надежной децентрализованной платформы голосования невозможно по причине отсутствия надежного механизма цифровой идентификации. Для решения данной проблемы возможно изучение опыта Эстонии, которая успешно решила данную задачу [3].

Список источников:

1. Блокчейн и децентрализованные системы : учеб. пособие для студ. заведений высш. образования : в 3 частях. Ч. 1 / П. Кравченко, Б. Скрябин, О. Дубинина. – Харьков : ПРОМАРТ, 2018. – 441 с.
2. Van Saberhagen N. CryptoNote v 2.0 [Электронный ресурс] / Nicolas van Saberhagen. – Oct. 2013. – Режим доступа: https://cryptonote.org/whitepaper.pdf.
3. D. Springall. Security Analysis of the Estonian Internet Voting System / Drew Springall, Travis Finkenauer, Zakir Durumeric. – University of Michigan, Ann Arbor, MI, U.S.A., 2011, – 13 с.