Опыт и перспективы электронного голосования

Окончание.
Начало в №2 от 4 февраля 2019 года

Идея проведения выборов на базе технологии блокчейн в настоящее время существует и развивается преимущественно в теоретическом аспекте. Однако анализ существующих концепций и предложений позволяет смоделировать системы электронного голосования на выборах на базе блокчейна и выдвинуть предложения о возможности их реализации.

Верификация и анонимность

Наиболее распространенной является универсальная модель, согласно которой выборы на блокчейне проходят так же, как и сделка с помощью криптовалют.

Каждый избиратель получает виртуальную монету, приравненную к голосу, и переводит ее на счет, связанный с кандидатом или партией. Привязка монеты к голосу осуществляется с помощью технологии colored coins, или цветных, окрашенных монет. С ее помощью монету можно привязать к любому активу, в том числе к голосу избирателя. После окончания голосования поступление монет на счета прекращается, количество монет соответствует количеству голосов. Таким образом, результаты выборов известны сразу.

Идентификация избирателя в системе наиболее предпочтительна через специально созданный интернет-сайт или приложение. При этом необходимо обеспечить соблюдение принципа тайного голосования. Указанное возможно с помощью протокола слепой подписи. Слепая подпись (blind digital signature) – это одна из модификаций электронной подписи, при которой подписывающая сторона достоверно не знает содержание подписываемого документа. Она зачастую используется в банковской сфере. Ее сущность заключается в том, что лицо, осуществляющее, к примеру, перевод денежных средств, удостоверяет свою личность с помощью электронной подписи. Система подтверждает идентификацию, однако банк видит только подтверждение платежа, но не персональные данные лица, что позволяет оставаться ему анонимным. В то же время в случае судебного разбирательства лицо может доказать факт совершения платежа.

В избирательном процессе лицо получает возможность верифицировать свою личность, оставаясь анонимным для избирательных комиссий и всех третьих лиц. Оно сможет отследить свой голос, но никто не увидит принадлежность данного голоса ему.

Кроме предложенного, существует протокол Биткойн ZeroCoin. Он был разработан с целью предоставления полной анонимности владельцам криптовалют. Разработчики говорят о том, что пользователи могут конвертировать с помощью криптографических методов неанонимную монету в анонимную, что не мешает ее передаче.

Другая модель электронного голосования с помощью технологии блокчейн была описана авторами статьи A Smart Contract for Boardroom Voting with Maximum Voter Privacy. С использованием разработанной ими системы был проведен локальный эксперимент. Авторы назвали используемую систему Open Vote Network. Голосование проходит в несколько этапов. Администратор системы составляет списки избирателей, верифицирует их, а также устанавливает временные рамки для каждого этапа голосования. После этого избиратели регистрируются в системе и голосуют, при этом их голос шифруется. После окончания голосования администратор уведомляет об этом систему и дает команду для подсчета голосов.

Эксперимент показал работоспособность системы, но одновременно выявил ряд технических недостатков. Среди них: отсутствие поддержки технологий шифрования, ограниченность объема памяти для записи результатов голосования, отсутствие средств поддержания работоспособности системы и ограничение максимального количества избирателей.

Еще одна модель разработана студентами Плимутского университета. Она не заменяет иные формы голосования, а скорее интегрируется в существующую систему. В ее рамках избиратель в первую очередь проходит регистрацию: через веб-страницу он представляет свои персональные данные для подтверждения личности в системе, которые формируются в блок информации. Данная транзакция анализируется так называемым государственным майнером, который создает новые блоки в блокчейн-цепочке данных об избирателях. Он принимает решение о том, прошел ли пользователь проверку. В случае подтверждения идентификации майнер отправляет избирателю специальную карточку и пароль для голосования.

Структурно система голосования располагается на местном, избирательном и федеральном уровнях. На местном уровне располагаются все цифровые избирательные участки, на избирательном уровне – устройства, принадлежащие избирателям, а на национальном уровне обеспечивается поддержка всей системы и создание цепи блоков. Все данные подвергаются зашифровке до окончания голосования.

Голосование начинается с идентификации избирателя в системе, после чего он получает доступ к веб-странице для голосования, которая у каждого избирательного округа своя. Система проверяет, что избиратель отдает свой голос впервые, после чего он осуществляет волеизъявление в виде выбора варианта ответа. Данная информация шифруется и поступает в систему, создавая новый блок. В избирательный участок приходит информация о поступлении данного голоса в систему, после чего необходимо удалить блок информации с данными об избирателе, представленными им при регистрации. Таким образом, параллельно существует цепь блоков с данными голосования и цепь с данными избирателей.

Преимущество данной системы заключается, прежде всего, в выделении различных взаимодействующих уровней, каждый из которых решает свою задачу. Также с положительной стороны следует отметить методы шифрования, предлагаемые авторами. Однако в данной модели больше недостатков: система идентификации пользователей получается весьма громоздкой. Необходимость участия государственного майнера отчасти лишает смысла использование технологии блокчейн, так как она сама по себе должна заменять любых посредников.

Неясно, каким образом после голосования можно удалить блок с персональными данными из блок-цепи, если технология блокчейн не предоставляет такую возможность. Авторы утверждают, что таким образом обеспечивается анонимность и тайна голосования, однако есть более эффективные и простые способы для этого. Кроме того, ведение двух блокчейн-цепей одновременно потребует в два раза больше энергетических затрат.

Слепая подпись

Еще в одной работе An E-voting Protocol Based on Blockchain авторы предлагают использовать модель, основанную на сочетании технологии слепой подписи и блокчейна. По принципу действия она схожа с универсальной моделью.