

## РЕЦЕНЗИЯ

на выпускную квалификационную работу обучающегося СПбГУ

Скаредова Сергея Антоновича

по теме

### «Реализация протокола электронного голосования на блокчейне Hyperledger Fabric»

Ставшая широко известной в последние несколько лет технология блокчейн предлагает новый способ децентрализованного взаимодействия различных субъектов, решающий проблему доверия во взаимодействиях между этими субъектами без единого доверенного узла, на основе консенсуса участников сети. Существуют задачи, для которых это свойство является существенным, что вызывает естественное желание предложить решения этих задач с использованием новой технологии.

Одной из таких задач является задача реализации голосования, в которой крайне важными являются как требование к отсутствию доверенного центра, чьи решения не могут быть проверены, так и требования по соблюдению тайны голосования. Одним из решений этой задачи, в применении к акционерным голосованиям является протокол e-Voting, реализация которого является темой данной работы. Задача акционерного голосования может рассматриваться как расширение задачи электорального голосования за счет наличия промежуточных узлов распределения голосов (депозитариев), различным числом голосов у различных участников, а также различными видами вопросов, по которым необходимо принять решение.

Реализация, выполненная Скаредовым С.А., является не первой реализацией данного протокола. Имевшаяся на момент начала работы реализация была максимально блокчейн-независимой, что имело как положительные (легкость адаптации для произвольного блокчейна), так и отрицательные (не возможность эффективно использовать все возможности конкретной платформы) стороны. Разработанная автором работы реализация отличается от исходной тем, что в ней максимально использованы особенности и возможности платформы Hyperledger Fabric.

Следует отметить, что это одна из самых сложных современных блокчейн-платформ, в некотором роде конструктор блокчейнов, содержащая различные специфические виды узлов сети и блоки для построения различных схем взаимодействия между элементами системы. Дополнительную сложность вызывает отсутствие хороших средств отладки и тот факт, что платформа всё еще находится в состоянии активного развития, т.е. содержит ошибки как в коде, так и в документации, которые, к тому же, непрерывно меняются.

Задача Сергеем Антоновичем была выполнена, но, к сожалению, работа обладает рядом недостатков, не позволяющих, на мой взгляд, признать ее полностью успешной и оценить на «отлично». Наиболее существенные из недостатков приведены ниже:

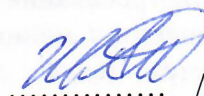
1. В тексте работы недостаточно полно отражены особенности акционерного голосования (и его отличия от электорального), а также используемых криптоалгоритмов (например, что именно понимается под отрицательными числами в кольце вычетов по модулю и что обозначается термином "аддитивность" в применении к монетам). Кроме того, не указано соответствие сущностей-участников реальным субъектам (или их ролям) в бизнес-процессе.
2. Из текста работы неясно, какие именно архитектурные особенности реализации представляются автору значимыми результатами его работы, а какие – непосредственно следуют из формулировки задачи.

3. Из работы неясно, какие из проверок, вынесенных в код смарт-контрактов, выполняются на всех узлах сети, а какие – на одном или на некоторых. Без этой информации трудно оценить, какой эффект в плане защиты от атак некорректными сообщениями даст предложенная архитектура.
4. Результаты нагрузочного тестирования позволяют сделать вывод только о соотношении скорости работы библиотек, используемых для реализации арифметики над эллиптическими кривыми на языках Go и Java (что, впрочем, отмечено автором). Неясно, что именно эти результаты могут сказать о представленном решении.

Считаю, что, несмотря на указанные недостатки, Скардовым С.А. в ходе выполнения работы была решена сложная инженерная задача в активно развивающейся области разработки ПО, и полученных результатов достаточно для того, чтобы оценить работу на 4 («хорошо»).

05.06.2020 г.

К. ф.-м. н., технический директор филиала частной акционерной компании с ограниченной ответственностью «ДиЭсЭкс ТЕХНОЛОДЖИЗ ЛИМИТЕД» ДиЭсЭкс Технолоджиз Раша



..... /Иванов А. Н./