УДК 316.776

Н.А. Северинчик, магистрант; Д.В. Шиман, доц., канд. техн. наук
(БГТУ, г. Минск)

АЛГОРИТМЫ ДОСТИЖЕНИЯ КОНСЕНСУСА МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ В СЕТИ BLOCKCHAIN

Консенсус – представляет собой процесс, посредством которого сеть компьютеров может дойти к однозначному решению, основной целью которого является уменьшение риска создания альтернативного блокчейна, закрытие сети или цензуры некоторых пользователей. Самыми популярными алгоритмами достижения консенсуса являются: PoW (Proof-of-Work/Доказательство работой) и PoS (Proof-of-Stake/Доказательство владением), за счет которых обеспечивается надежность и устойчивость.

Основными минусами данных алгоритмов являются:

Относительно PoW, огромные расходы: требуется оборудование с очень большой вычислительной мощностью для корректной работы системы. Вычисления, которые производятся для работоспособности системы, создавая блоки, потребляют огромное количество электроэнергии, и вычисления, которые они делают, совершенно бесполезны сами по себе, да, они гарантируют безопасность в сети, но их результаты нельзя использовать в бизнесе или в науке. Возможность атаки 51%: если в руках злоумышленника находится больше половины всех вычислительных мощностей в сети, то у него появляется возможность подтверждать только свои блоки, при этом игнорируя чужие, становясь «главным управляющим узлом».

В PoS также присутствует проблема атаки 51%, в случае, когда небольшая группа пользователей соберёт необходимое количество токенов сети она сможет навязывать свои правила работы сети остальным участникам . Также возможна децентрализация сети, если у одного из участников будет больше чем 50% всех токенов.

Изучив основные проблемы популярных алгоритмов консенсуса была предложена концепция нового алгоритма, базирующегося на понятии «кредитная история».

Узлу сети разрешается создать блок с транзакциями, в случае, когда между узлами, которыми производилась транзакция, «история» положительна. «История» является положительной, если остальные узлы проверили что все правила для проведения транзакции соблюдены, чем больше верифицированных транзакций между узлами, тем меньше подтверждений требуется от остальных участников сети. Таким образом решается проблема возможной «атаки 51%».