УДК 004.75

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ ПРОТОКОЛОВ КОНСЕНСУСА POW И DPOW

Филипенко Д.А. (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)

Научный руководитель – к.т.н., доцент Бибиков С.В.

(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)

Аннотация. Алгоритмы достижения консенсуса – математические алгоритмы, позволяющие всем пользователям сети прийти к общему согласию относительно определённого ключевого момента для того, чтобы блокчейн оставался децентрализованным. В работе проведен сравнительный анализ безопасности протоколов доказательства работы (далее – PoW) и отложенного доказательства работы (далее – dPoW).

Введение. Блокчейн – последовательность блоков данных, связанных с предыдущей частью каждого блока. Новые блоки добавляются в конец цепочки. Одной из главных проблем технологии блокчейн является достоверность данных, что определяет необходимость применения эффективных алгоритмов шифрования. Однако не менее важен вопрос специальных алгоритмов конкурентного доступа, разрешения коллизий в сети, достижения согласия. Процесс достижения консенсуса стал бы невозможным без алгоритма, который способен автоматически проверять новые транзакции. Без подходящего алгоритма, децентрализованные системы должны были бы уступить централизованному источнику, хранящему и обрабатывающему данные в одном месте. Таким образом информация, которую он хранит, стала бы уязвимой для атак и иных неправомерных действий тех, кто сможет получить доступ к его местоположению. На данный момент существует более десяти алгоритмов достижения консенсуса в блокчейне. Выбор протокола консенсуса зависит от типа используемого распределенного реестра. В контексте данной работы рассмотрена безопасность одного из популярных алгоритмов – PoW и его модификации – dPoW.

Основная часть. Основой технологии распределенного реестра является протокол консенсуса. Протокол консенсуса – это некий механизм, набор правил, с помощью которых сеть приходит к согласию. Другими словами, набор правил, с помощью которых узлы согласовывают валидацию транзакций. Поэтому протоколы консенсуса также могут быть названы протоколами согласия. Основная роль алгоритмов согласия заключается в достижении высокого уровня надежности сети, построенной на серии узлов, т. е устройств, соединённых с другими устройствами как часть компьютерной сети. Другими словами, если совершена транзакция – алгоритм начнет работать (обмениваться данными по сети для проверки, может ли иметь место данное действие). Сам процесс принятия решений называют консенсусным алгоритмом (протоколом). При проектировании таких протоколов особое внимание уделяется вопросам децентрализации и анонимности. Алгоритм согласия имеет ряд целей, таких как согласование, инклюзивность, кооперативность, эгалитаризм. Данные аспекты стоит рассматривать с нескольких сторон. Со стороны эффективности (скорости и сложности консенсусных алгоритмов), надежности (задача византийских генералов) и со стороны безопасности (стойкости к известным атакам на протоколы согласия). Именно вопрос безопасности алгоритмов согласия рассмотрен в данной работе. Протокол PoW – один из наиболее популярных алгоритмов консенсуса, использующийся для согласования цепочки блоков. Однако, PoW имеет ряд недостатков. В свою очередь dPoW не является основным механизмом достижения консенсуса. Это механизм согласия второго уровня, который в свою очередь обеспечивает высокий уровень безопасности в дополнение к существующим

алгоритмам консенсуса. В ходе исследования данных алгоритмов согласия выявлены особенности данных алгоритмов с точки зрения их применения и безопасности.

Выводы. Алгоритм отложенного доказательства работы решает проблему возникновения атаки 51%. Также он может быть добавлен как вторичный уровень консенсуса к существующему консенсусному алгоритму. Например, его можно добавить в качестве вторичного консенсуса в блокчейны, которые используют традиционный протокол доказательства работы – PoW или протокол доказательства доли Prof of Stake. Таким образом, dPoW может быть использован для повышения безопасности для любого блокчейна, используя данный алгоритм консенсуса.

Филипенко Д.А. Подпись

Бибиков С.В. Подпись