КРИПТОГРАФИЯ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Н.В. Яковчик

Криптография – это основа технологии блокчейн, обеспечивающая его стабильную работу. Участники сети могут доверять друг другу, т.к. это гарантируется математически. Этому способствуют такие фундаментальные элементы блокчейна, как хеш-функции и электронно-цифровые подписи [1].

Хэш-функция – это детерминированная функция, на вход которой подается строка битов произвольной длины, а выходом всегда является битовая строка фиксированной длины *n*. Блокчейн состоит из блоков, каждый из которых имеет хэш предыдущего блока. Таким образом получается цепочка связанных объектов. Если какой-то из блоков будет модифицирован, то его хэш не совпадет со значением, записанным в следующем блоке, что будет является признаком вмешательства в систему.

Помимо защиты блоков, хеширование используется в механизме консенсус, который позволяет определить того, кто сможет добавить новый блок в цепочку. Для добавляемого блока выставляется определенное требование к виду его хэша, например, пять последних символов должны быть нулями. Так как изначально нельзя подобрать данные для получения нужного кэша, единственный вариант – это перебор. В новом блоке создается поле (nonce), значение в котором изменяют до тех пор, пока не будет получен нужный хэш.

Для защиты транзакции применяется криптографическая система с открытым ключом [2] (электронно-цифровая подпись). Публичный ключ является номером кошелька, на адрес которого могут отправляться транзакции, которые в свою очередь должны быть подписаны приватным ключом для проверки личности отправителя.

Литература

1. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. – М.: Эксмо, 2018. – 256 с.

2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009 – 576 с.