УДК 512.624.95

КРИПТОГРАФИЯ В БЛОКЧЕЙНЕ

Васильков В.С. и Рогожник Я.А.

Научный руководитель – Катковская И.Н., к. ф-м. н., доцент

Проблема защиты информации с каждым годом становится всё более востребованной. Практически повсеместное использование шифров нуждается в защите от хакеров, которые, в частности, могут вносить изменения в банковские системы. Позволяют же бороться с ними блокчейн-технологии.

Блокчейн основывается на принципах свободного просмотра. Выделяются открытые и закрытые системы, но их объединяет общая система построения. Блокчейн представляет собой последовательность, в которой каждый блок связан с предыдущим. Этому способствуют такие фундаментальные элементы блокчейна, как хеш-функции и электронно- цифровые подписи.

Хеширование — это процесс, преобразовывающий входные данные произвольной длины в битовую строку определенной длины, при этом выходная хеш-функция заполняется различными символами.

Рисунок 1. Пример работы хеш-функции

Из примера следует, что имея различные тексты, как пример информации и применяя к ним алгоритмы хеширования - на выходе мы получаем хеш одинакового размера, но заполненный разными символами. Хеш-функции нужны для связывания блоков в блокчейне, что позволяет обращаться к ним и просматривать их.

Цифровые подписи — это способ доказать, что вы являетесь владельцем ячейки блокчейна. Принцип работы блокчейна приведён ниже.

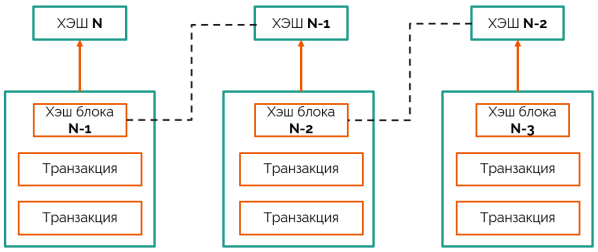

Рисунок 2. Структура Блокчейна

Системы шифрования, которые используют принцип двух ключей: открытого, который является адресом пользователя и закрытого, который является скрытым и нужен для дешифровки данных. Само шифрование проводится по схеме Эль-Гамаля и использует уже готовые алгоритмы.

Следует заметить, что любой абонент, знающий открытый ключ абонента, может посылать ему сообщения. Но не каждый абонент сможет расшифровать эти сообщения.

Таким образом мы продемонстрировали все возможности криптографии и технологии блокчейна в современных реалиях. За системами с открытым ключом и блокчейн технологиями стоит будущее современной криптографии. Данные системы в совокупности могут дать большой толчок в развитии науки и экономики.

Литература

1. https://habr.com/ru/company/bitfury/blog/327272
2. «Алгоритмы шифрования» Панасенко С.П. 2009 г.
3. http://crypto-r.narod.ru/glava6/glava6_3.html