ЛОГИСТИЧЕСКАЯ МОДЕЛЬ «ДОСТОВЕРНОСТИ» ТЕХНОЛОГИИ БЛОКЧЕЙН

А.В. Сидоренко, М.Г. Волосач

Белорусский государственный университет, Минск, Беларусь

Одной из основных проблем применения технологии блокчейн является достоверность данных, что определяет необходимость применения эффективных алгоритмов шифрования. Они должны гарантировать достаточную криптографическую стойкость для информации в сети, а также обеспечить реализацию цифровой подписи при необходимости.

В работе для шифрования рассматривается алгоритм ассимметричного щифрования RSA. Алгоритм использует два ключа: открытый и секретный, которые вместе образуют пару ключей. Если сообщение было зашифровано открытым ключом, то расшифровать его можно ключом, известным только получателю переданной информации. При попытке взломать секретный ключ придется перебрать достаточно много комбинаций Например, при длине ключа в 256 бит и скорости подбора паролей 1024 в секунду потребуется перебрать 1,23+67 лет.

Нами предложен функционал программного продукта, предназначенного для обработки и анализа информации. Реализация программы проведена на языке C++.

Приводится пример работы компьютерной программы. Разработанный программный продукт обладает достаточно низкими системными требованиями. Особенностью данного программного продукта является возможность работы с мобильным телефоном.

Широкое распространение технологии «Интернет вещей» в различных сферах человеческой деятельности вызывает необходимость в обеспечении ключевых факторов: секретности, конфиденциальности, аутентификации передаваемой информации. Для сохранения связи между датчиками распределенных на большой территории пользователей и обеспечения достоверной передачи данных к облачным технологиям в настоящее время получают распространение системы на основе блокчейна и краевые вычисления [1]. Такие характеристики блокчейна, как: децентрализация, механизм консенсуса, шифрование данных и смартконтракты позволяют сохранить в базе данных и обеспечить конфиденциальность и аутентификацию передаваемой информации.

Нами предложен функционал программного продукта, предназначенного для получения, обработки и анализа информации с датчиков, совместимых с платой Arduino. Разработанный программный продукт обладает достаточно низкими системными требованиями и может быть запущен с использованием пакета Java, в частности, версии Java Runtime Envirioment. Особенностью данной системы является возможность работы с мобильным телефоном. При этом информация может быть передана на телефон и получена в виде сообщения электронной почты на компьютере.

Список литературы

1. Сидоренко А.В. Робототехника и блокчейн // Развитие информатизации государственной системы научно-технической информации: матер. XVII Междунар. конф., Минск, 20 сентября 2018 г. С. 111–114.