БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра технологий программирования

Аннотация к дипломной работе

«Организация защищенных транзакций на основе протокола с нулевым разглашением»

Проценко Артем Андреевич

Научный руководитель – кандидат технических наук, доцент кафедры технологий программирования Войтешенко И. С.

Минск, 2021

РЕФЕРАТ

Дипломная работа, с.46, рис.16, 6 формул, 12 источников.

Ключевые слова: ПРОТОКОЛ НУЛЕВОГО РАЗГЛАШЕНИЯ, ZK-SNARK, БЛОКЧЕЙН.

Объект исследований–протокол нулевого разглашения, блокчейн, компилятор circom.

Предмет исследований – применение протокола нулевого разглашения для создания защищенных транзакций.

Цель работы – реализовать блокчейн приложение, основанное на защищенных транзакциях.

В результате исследования изучены существующие виды протоколов нулевого разглашения, изучен каркас блокчейна, разработан способ организации защищенных транзакций в блокчейн приложении.

Методы исследования – работа над проектом децентрализованного приложения

Областью применения является промышленная разработка децентрализованных приложений с использованием библиотеки snarkjs.

РЭФЕРАТ

Дыпломная работа, с. 46, мал. 16, 6 формул, 12 крыніц.

Ключавыя словы: ПРАТАКОЛ НУЛЯВОГА ВЫДАВАННЯ, ZK-SNARK, БЛОКЧЭЙН.

Аб'ект даследаванняў: пратакол нулявога выдавання, блокчэйн, кампілятар circom.

Прадмет даследаванняў – прымяненне пратаколу нулявога выдавання для стварэння абароненых транзакцый.

Мэта работы: рэалізаваць блокчэйн прыкладанне, якое выкарыстоўвае абароненыя транзакцыі.

У **выніку даследавання** вывучаны існуючыя віды пратаколаў нулявога выдавання, вывучаны каркас блокчейна, распрацаваны спосаб арганізацыі абароненых транзакцый у блокчейн прыкладанні.

Метады даследавання: праца над праектам дэцэнтралізванага прыкладання.

Вобласцю ужывання з'яўляецца прамысловая распрацоўка дэцэнтралізаваных прыкладанняў з выкарыстаннем бібліятэкі snarkjs.

Abstract

Diploma project, 46p., 16 pic., 6 formulas, 12 sources.

Keywords: ZERO-KNOWLEDGE PROTOCOL, ZK-SNARK, BLOCKCHAIN.

Object – zero-knowledge protocol, the blockchain, and the circom compiler.

Subject – application of zero-knowledge proof for creating shielded transactions.

Work goals: implementation of a blockchain application that uses shielded transactions.

Results: examined the existing types of zero-knowledge protocols, the blockchain architecture was studied, and a method for organizing shielded transactions in a blockchain application was developed.

Methods of research: working on a project of a decentralized application.

Scope: development of decentralized applications using the snarkjs library.