

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе
АНАЛИЗ И РЕАЛИЗАЦИЯ КРИПТОВАЛЮТЫ

Гончар Евгений Олегович

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

2019

В дипломной работе содержится:

- 56 страниц
- 4 рисунка
- 2 таблицы
- 6 источников
- 1 приложение

Ключевые слова: BITCOIN, БЛОКЧЕЙН, RIPEMD-160, Secp256k1, SHA-256, ECDSA, ЭЛЛИПТИЧЕСКАЯ КРИВАЯ, ХЕШ-ФУНКЦИЯ, ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ, КРИПТОВАЛЮТА

В ходе выполнения дипломной работы изучался вопрос криптографической составляющей криптовалюты и ее архитектуры.

В качестве целей для данной дипломной работы были поставлены изучение и реализация криптографических алгоритмов, используемых в криптовалюте Bitcoin, ее описание и реализация архитектуры.

Достижение поставленной цели достигалось через:

- Изучение разделов криптографии
- Изучение официальной документации криптовалюты Bitcoin

В дипломной работе представлены реализации следующих алгоритмов: RIPEMD-160, SHA-256, ECDSA, - а также функции для работы с цепочкой блоков, блоками, транзакциями и адресами пользователей.

Дипломная работа выполнена автором самостоятельно.

The graduation paper consist of:

- 56 pages
- 4 images
- 2 tables
- 6 sources
- 1 attachment

Keywords: BITCOIN, BLOCKCHAIN, RIPEMD-160, Secp256k1, SHA-256, ECDSA, ELLIPTIC CURVE, HASH FUNCTION, DIGITAL SIGNATURE, CRYPTOCURRENCY

The question of the cryptographic components of the cryptocurrency and its architecture was studied.

The goal of the graduation paper is to implement cryptographic algorithms used in Bitcoin cryptocurrency and its architecture.

This goal is achieved through:

- Studying of cryptographic sections
- Studying official documentation of Bitcoin

In the graduation paper presents the implementation of the following algorithms: RIPEMD-160, SHA-256, ECDSA, - as well as functions for working with a blockchain, blocks, transactions and addresses of users.

The graduation paper is made by the author himself.