https://lms.hse.ru/?apview&h_id=DFF87B12-06AD-4B8A-87FB-245089F1268E

ФИО:	Куприянов Кирилл Игоревич
Руководитель:	Авдошин Сергей Михайлович, профессор, доцент
Факультет:	Факультет компьютерных наук
Кафедра/Группа:	М ФКН БПИ151
Уровень обучения:	Бакалавриат
Образовательная программа:	Программная инженерия
Адрес электронной почты:	kupriyanovkirill@gmail.com
Контактный телефон:	+7(910)008-39-26
Название (тема) по-русски:	Криптографические алгоритмы и протоколы для распределенных реестров
Название (тема) по-английски:	Cryptographic Algorithms and Protocols for Distributed Ledgers
Язык работы:	Русский
Процент заимствования:	4
Дата загрузки работы:	22-05-2019 12:04:20

Аннотация:
Технология блокчейн обычно ассоциируется с криптовалютой биткойн, потому что биткойн - первая повсеместно используемая система, использующая блокчейн как основу. По мере развития технологий число различных блокчейнов со множеством способов их приложения резко возросло. Факт существования такого значительного их количества можно объяснить тем, что при их реализации могут варьироваться используемые криптографические алгоритмы и протоколы. В связи с этим возникла проблема отсутствия систематически собранной и структурированной информации о криптографических алгоритмах и протоколах в существующих распределенных реестрах. Главной целью данной работы является сбор и обобщение известных и распространенных на сегодняшний день криптографических алгоритмов и протоколов. Предложен сравнительный анализ алгоритмов, используемых в блокчейнах, по общим показателям. Также в качестве инструмента для разработчиков при создании персонального распределенного реестра в образовательных целях разработана библиотека на языке Python3.6, в которой собраны реализации проанализированных алгоритмов и протоколов.

Ключевые слова ——- блокчейн, биткоин, распределённый реест, технология распределённого реестра, криптография, классификация, Python.

Аннотация (англ.):
The Blockchain technology is typically associated with Bitcoin, because it was the first system which has been distributed using the Blockchain technology. As the technologies evolved, the number of various blockchains with different kinds of applications had been drastically risen. A huge amount of blockchains

can be explained by various cryptographic algorithms and protocols usage in them. It brought a problem of the absence of systematically gathered and structured information about cryptographic algorithms and protocols in existing distributed ledgers. The main objective of this work is to generalise all known common cryptographic algorithms and protocols, which are being used nowadays. The algorithms used in blockchains are going to be classified by common metrics: time complexity, space complexity, and the resistance to hacking. It is also intended to bring a programming library in Pyhon3.6, where analyzed algorithms and protocols are gathered in one place. The library would serve as a toolbox for developers when creating a personal distributed ledger.

Index terms ——- blockchain; bitcoin; distributed ledger; DLT; cryptography; classification; python

Я подтверждаю, что выпускная квалификационная работа выполнена мною лично и:

1. не воспроизводит мою собственную работу, выполненную ранее, без ссылки на нее в качестве источника;
2. не воспроизводит работу, выполненную другими авторами, без указания ссылки на источник учебной или научной литературы, статьи, вебсайты, выполненные задания или конспекты других студентов;
3. не предоставлялась ранее на соискание ступени более высокого уровня;
4. содержит правильно использованные цитаты и ссылки;
5. включает полный библиографический список ссылок и источников, которые были использованы при написании работы.

Мне известно, что нарушение правил цитирования и указания ссылок рассматривается как обман или попытка ввести в заблуждение, а также квалифицируется как нарушение Правил внутреннего распорядка НИУ ВШЭ.

Я разрешаю / ~~отказываюсь по причине~~(нужное оставить)

(указать причину отказа в публикации)

НИУ ВШЭ безвозмездно воспроизводить и размещать (доводить до всеобщего сведения) в полном объеме написанную мною в рамках выполнения образовательной программы выпускную квалификационную работу (бакалавра/дипломную работу/магистерскую диссертацию) с указанием моего авторства и даты выполнения работы, а также данных о научном руководителе моей работы, в сети Интернет на корпоративном портале (сайте) НИУ ВШЭ, расположенном по адресу www.hse.ru, таким образом, чтобы любой пользователь данного портала мог получить доступ к полному тексту выпускной квалификационной работы из любого места и в любое время по собственному выбору.

Дата: 22-05-2019

Подпись: