



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Факультет Компьютерных Наук
Департамент Программной Инженерии
Выпускная квалификационная работа

Криптографические алгоритмы и протоколы для
распределенных реестров
Cryptographic Algorithms and Protocols for Distributed Ledgers

Выполнил: студент гр.БПИ151 Куприянов Кирилл
Научный руководитель: Профессор, руководитель ДПИ,
к.т.н. Авдошин Сергей Михайлович

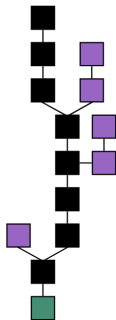
2018

1. Распределённые реестры – база данных, которая распределена между несколькими сетевыми узлами или вычислительными устройствами. Каждый узел получает данные из других узлов и хранит полную копию реестра. Обновления узлов происходят независимо друг от друга

2. Криптография – наука, изучающая математические методы защиты информации, методы преобразования, обеспечивающие ее конфиденциальность и аутентичность.

Разделы: асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции

- Симметричное шифрование — для шифрования и расшифровывания применяется один и тот же криптографический ключ
- Асимметричное шифрование — открытый ключ передаётся по открытому каналу и используется для проверки ЭП и для шифрования сообщения
- Электронная подпись (ЭП) — электронный документ, полученный преобразованием закрытым ключом подписи. Позволяет проверить *целостность, авторство и неотказуемость*



Блокчейн



Криптовалюты

Цель: проделать анализ основных и наиболее распространённых криптографических алгоритмов для распределённых реестров в мире.

Задачи:

- Выявить популярные распределённые реестры; выделить и изучить криптографические алгоритмы в них
- Замерить параметры алгоритмов
- Классифицировать их по:
 - Времени работы
 - Эффективности по памяти
 - Количеству операций в секунду
- Сделать обзор лучших алгоритмов по приведённым параметрам
- Написать библиотеку классов с содержанием криптографических алгоритмов

Исследовательская часть

- Изучение и анализ криптографических алгоритмов в блокчейнах
- Изучение и анализ криптографических алгоритмов в распределённых реестрах, не являющимися блокчейнами
- Сравнение российского MasterChain с зарубежными аналогами

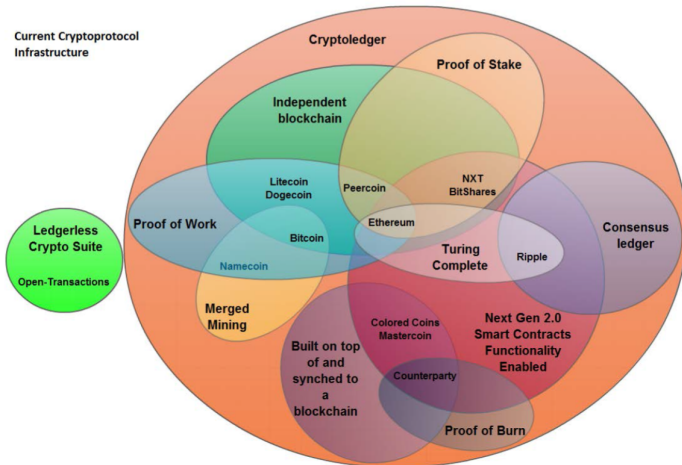
Практическая часть

- Составление библиотеки классов, содержащую:
 - Алгоритмы хэширования
 - Алгоритмы цифровых подписей
- Библиотеку классов можно использовать для упрощённого создания распределённого реестра, например, блокчейна

Существующая классификация криптопротоколов

На 2014 год

Задача: Расширение классификации



- Сравнительный анализ
- Язык Python
- \LaTeX для презентаций и текста



- [1]: **Swanson, T.** (2014) *Great Chain of Numbers a Guide to Smart Contracts, Smart Property and Trustless Asset Management*
- [2]: **Satoshi N.** (2007) *Bitcoin: A Peer-to-Peer Electronic Cash System*
- [3]: **Aladin, D.** (2017) *Blockchain Documentation*
- [4]: **Cryptocurrency** (2018) <https://en.wikipedia.org/wiki/Cryptocurrency>

Факультет Компьютерных Наук
Департамент Программной Инженерии
Выпускная квалификационная работа

Выполнил: студент гр.БПИ151 Куприянов Кирилл
Научный руководитель: Профессор, руководитель ДПИ,
к.т.н. Авдошин Сергей Михайлович

2018