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

Предметная область

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

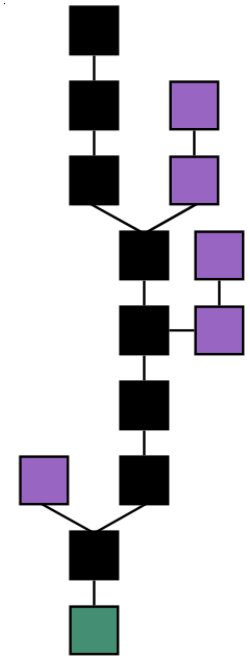
2. Криптография – наука, изучающая математические методы защиты информации, методы преобразования, обеспечивающие ее конфиденциальность и аутентичность.
Разделы: асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции

Определения

- 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*

Обоснование актуальности работы

Популярность скидок в интернете



Блокчейн

Криптовалюты

Цель и задачи работы

Цель: Анализ и классификация актуальных 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 (сложности, time complexity)
  - Эффективности по памяти (space complexity)
- Сделать обзор лучших алгоритмов по приведённым параметрам
- Написать библиотеку классов с содержанием криптографических алгоритмов

Ожидаемые результаты

Исследование и практика

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

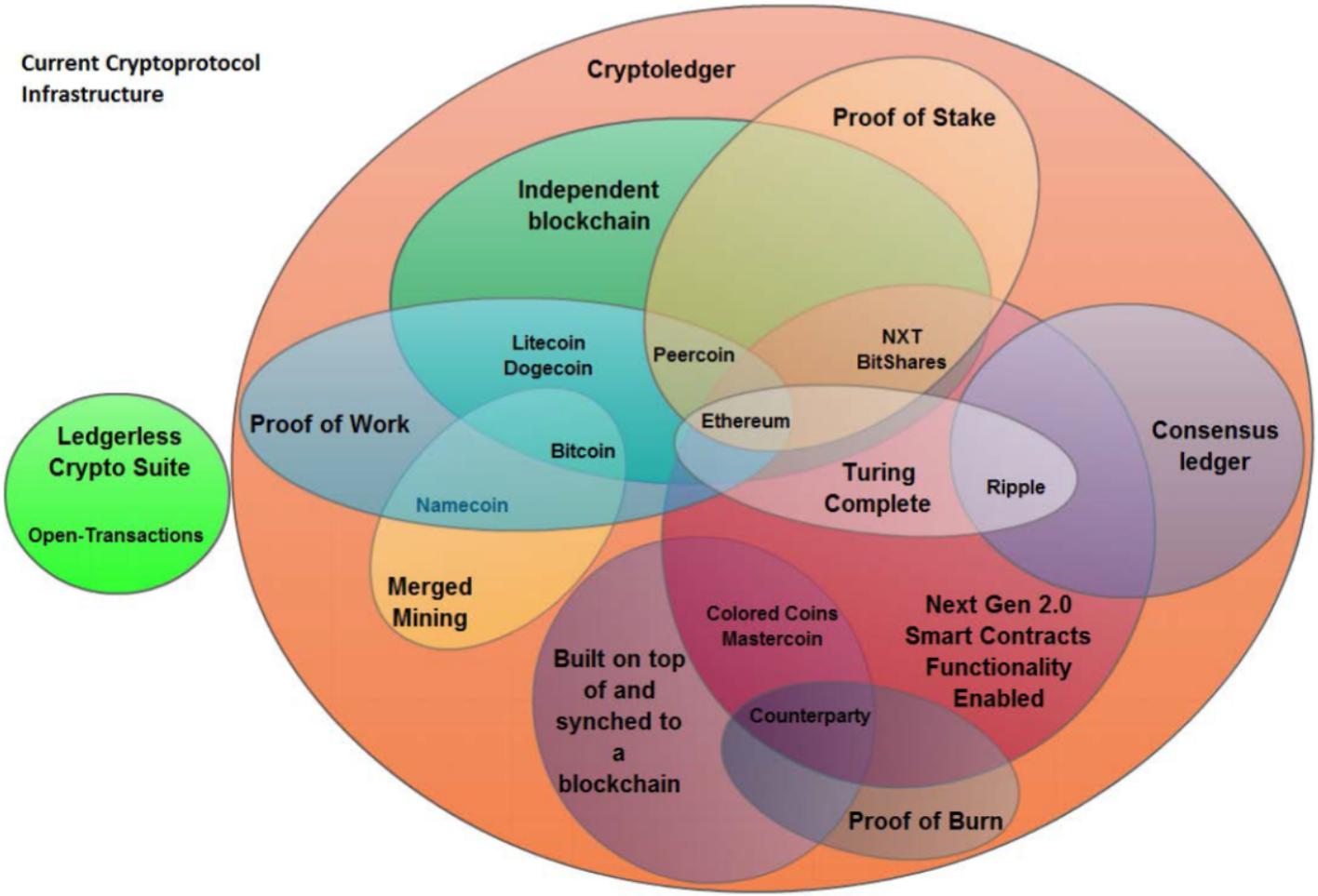
Практическая часть

- Формирование библиотеки классов на Python 3.6, 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



Методы, алгоритмы и технологии

- Сравнительный анализ алгоритмов и протоколов
- Язык Python 3.6
- LaTeX (дистрибутив XeTeX) для презентаций и текста

Список используемых источников

[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*

Спасибо за внимание!

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