

## Текст презентации

Добрый день, уважаемая комиссия, студенты. Меня зовут Куприянов Кирилл, и я занимаюсь исследованием криптографических алгоритмов и протоколов для распределённых реестров. Мой научный руководитель — Авдошин Сергей Михайлович.

---

Моя предметная область связана с популярной сегодня темой — криптовалюты, распределённый интернет, технология блокчейн, криптография. Очень много работа сейчас публикуется на эту тему, и с момента взятия темы сама область уже расширилась и нужно держаться постоянно в курсе чтобы не отстать от времени.

---

В процессе своего выступления я буду использовать технические термины, которые стоит сразу обозначить.

---

Оглавление ВКР, в главе 1 описана теоретическая база и описание рассмотренных технологий распределённых реестров. Это включает в себя алгоритмы и протоколы, и т.д.. В главе 2 проводится их анализ и строится классификация, а в третьей описывается построение программы.

---

Актуальность обоснована популярностью технологии блокчейн, отсутствием полной классификации криптографических алгоритмов, используемых для функционирования криптовалют, и необходимостью на сегодняшний день создать такую классификацию. Люди опираются на бизнес логику а не на реальные факты о реализации и надёжности, так же отсутствует библиотека/программа где всё посмотреть легко.

---

Вот так выглядит существующая классификация на сегодняшний день, она приведена в книжке [15] Она хорошая и достаточно полной была на 2014 год, но сейчас надо новое

---

Соответственно, я задался целью проделать анализ криптографических алгоритмов для популярных в мире распределённых реестров, и для этого мне необходимо было выявить какие алгоритмы используются в распределённых реестрах, сравнить их по времени работы и объёму памяти, выявить лучших. Это для анализа. А те алгоритмы, которые я собрал, исследуя распределённые реестры, я планирую объединить в одну общую библиотеку, так сказать, некий тулkit для экспериментирования с распределённым реестром.

---

Все распределённые реестры DL делятся на несколько типов на рисунке.

---

Реестры по открытости бывают разные. Зависит от того, какой классификации придерживаться. Мы будем российской. Цитаты: 17, 7, 19

---

В них используются алгоритмы и протоколы и это не полный список, руководствуясь поисками и наводками я искал и изучал информацию, составлял сравнительные таблицы и в итоге кое-что получилось

---

2 ПРОПУСКА СЛАЙДОВ СКАЖУ САМ. Для качественного сравнения нужно было найти необходимые ресурсы на каждый рассматриваемый реестр. Часть таблицы с источниками информации приведена на слайде.

Дальше сам тоже.