

## Текст презентации

Добрый день, уважаемая комиссия, студенты. Меня зовут Куприянов Кирилл, и сейчас я буду рассказывать про выбранную тему выпускной квалификационной работы, которую я буду выполнять и защищать в этом учебном году.

Тема: Криптографические алгоритмы и протоколы для распределенных реестров, а научный руководитель — Авдошин Сергей Михайлович.

---

Моя предметная область связана с популярной сегодня темой — криптовалюты, распределённый интернет, технология блокчейн, криптография. Сразу отмечу, что любой вид блокчейна это есть распределённый реестр, но существуют распределённые реестры, не являющиеся блокчейнами. Так, например, существует криптовалюта IOTA, криптографические алгоритмы которой основываются на ациклических графах, вместо дерева Меркля, как это устроено в остальных ранних блокчейнах.

---

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

---

Актуальность обоснована популярностью технологии блокчейн, отсутствием полной классификации криптографических алгоритмов, используемых для функционирования криптовалют, и необходимостью на сегодняшний день создать такую классификацию.

---

Соответственно, я задался целью проделать анализ криптографических алгоритмов для популярных в мире распределённых реестров, и для этого мне необходимо будет 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 классов, так сказать, некий тулkit для создания своего распределённого реестра, например, для учёта зарплат сотрудников фирмы, или запуска своей криптовалюты.

---

В ожидаемые результаты исследовательской части работы я также включил сравнение зарубежных блокчейнов с российским MasterChain'ом, интересно узнать их различия внутренней архитектуры, выделить сильные и слабые стороны, и включить в библиотеку технологии из мастерчейна.

---

В открытых источниках существует такая классификация, она на 2014 год. Данная классификация включает в себя на верхнем уровне 2 вида систем: на основе реестра, и те, в основе которых не лежит реестр, тут изображена только Open Transactions. Моей косвенной задачей ВКР будет расширить данную диаграмму, поскольку с 2014 года произошло серьёзное пополнение обеих систем, и интересно посмотреть, как вырастит данная диаграмма.

---

Используемые технологии на слайде.

---

А так же источники, которыми я руководствовался и использовал при создании презентации.

---

Спасибо за внимание! С удовольствием отвечу на ваши вопросы.

---