Текст презентации

Текущее десятилетие — интересное время развития децентрализованных технологий. Добрый день, уважаемая комиссия и коллеги-студенты, моя работа, которую я выполнял под руководством Сергей Михайловича, связана с криптографическими алгоритмами и протоколами для распределённых реестров. Стоит отметить заранее, что в работе не предлагаются реализации новых, доселе неизвестных алгоритмов. Поскольку благодаря усилиям, которые на протяжении предыдущих тридцати лет прикладывали криптографы, математики и кодировщики, разрабатывая строго специальные усовершенствованные протоколы для защиты конфиденциальности и гарантий аутентичности различных систем, дают возможность современным технологиям, утилизируя вычислительные мощности и применяя знания, усердно накопленные предыдущими поколениями, создавать необычайные распределённые системы.

Котрые приносят немалый доход. На данном графике виден текущий и будущий стабильный рост выручки в индустриях где применяется блокчейн.

Кроме того, актуальная новость: Ростех предложил перевести все гос информационные системы на технологию блокчейн, на что проект потребует серьёзных инвестиций.
На создание своей работы я был вдохновлён исследованием Тима Сэунсона, известного в кругах по интересу блокчейна публициста.

В процессе выступления будут использованы слудующие термины, с которыми Вы сможете ознакомиться не только на слайде, но и обратившись к раздаточному материалу.

В работе я стремился к обновлению существующей классификации и реализации идеи программного решения для создания кодов реестра.

В начале будет обозрена теоретическая часть работы, затем программная, и в конце будут подведены общие итоги по проделанному объёму.

Множество. научных. и публичных. источников. были. использованы. во время изучения темы распределённых реестров. Для глубокого понимания реализаций, были прочитаны статьи с ResearchGate и SpringerLink, а для получения актуальных обновлений и современных трендов, отслеживались публикации на тематических форумах и страницах.

Результатом теоретической части работы стало обновлённая классификация алгоритмов и протоколов для распределённых реестров. На слайде — старая. Автор Тим Суэнсон, 2014 год. Он постарался отразить на одной диаграмме полную картину по использованию определённых технологий в различных реестрах. К примеру, мистер Суэнсон выделяет 2 типа реестров: cryptoledger, и ledgerless cryptosuite.

В обновлённой классификации, были выделены новые, не существовавшие ранее реестры, а также пополнился обхват наименований алгоритмов и протоколов.

Всё многообразие алгоритмов и протоколов натолкнуло на мысль о том, что есть необходимость быстрого получения кодов реализаций алгоритмов, и не только. Приложение / библиотека, можно рассматривать как угодно, которое при моём желании встроить в своё приложение (учёт зар-

плат сотрудников организации, регистрирование государственных документов, или даже социальная сеть) логику блокчейна, давало бы мне возможность это сделать, предоставив код реализации блокчейна, при чём, используя те алгоритмы, которые выбрал я, опираясь на их данные по работе. Я, как пользователь, хочу иметь возможность получения готового кода блокчейна с использованием алгоритмов на мой выбор, чтобы встраивать его в другие свои приложения.

Программное решение, речь о котором пойдёт далее, имеет на сегодняшний момент 2 конкурентноспособных аналога, перед которыми данное решение выступает с рядом преимуществ.

На верхнем уровне, приложение построено из двух частей, которые были названы компоновщик, и реализация блокчейна.

Компоновщик работает следующим образом. Его процесс работы вы можете так же наблюдать в диаграмме последовательностей в раздаточном материале. Компоновщик на вход получает выбор конкретных алгоритмов, затем, используя остальные части реализации, предоставляет на выходе сгенерированный по указанному пути код реестра, в котором предусмотрен интерфейс встраивания вариаций алгоритмов.

Реализации алгоритмов, которые встраиваются в программу, были заимствованы из публичных источников (хотя некоторые из них, изначально наисанные на Питон2, необходимо было адаптировать под язык Питон3), в то время как остальные компоненты были реализованы самостоятельно.

Сценарии для пользователя относительно двух частей программ отражены, но лучше всего их покажет дальнейшая демонстрация.

Для поддержания консистентности программы, на отдельной хост-системе реализовано автообновление, насыщающее репозиторий свежими реализациями алгоритмов. Процессы CI автоматически не позволяют неработающим версиям алгоритмов попасть в репозиторий без контроля, а использование конфигурационного файла позволяет уменьшить количество аргументов командной строки.

Поддержание консистентности происходит посредством запуска скриптов обновления на сервере каждый день в 21:00.

В начале запускается скрипт, запрашивающий обновления из публичных источников, а позже — скрипт, который загружает полученные обновления и логи скриптов в репозиторий.

Для системы использовался язык Python версии 3.6.5, конфигурационные файлы были написаны на Yaml'e, процесс обмена сообщениями по http протоколу реализован при помощи библиотеки Flask. Была использован система контроля версий Git совместно с хостингом программных проектов Github, система continuous integration Shippable, библиотека matplotlib для отрисовки графиков, UNIX утилита crontab для задания расписания обновлений, а так же система вёрстки LaTeX для создания текста ВКР и презентации.

Демо на 5 минут

Подводя итоги, устаревшая классификация обновлена, а так же создано программное средство для генерации кодов реестров, и налажена автоматизированная система для обновления и работы с готовыми кодами реализаций алгоритмов. Так же, работа находится в публичном доступе.

В репозитории присутствуют дружелюбные инструкции по установке программы в систему и её использованию с примерами.

В качестве усовершенствования работы предлагаются следующие шаги.

Благодарю всех за внимание, и в ближайшее время готов ответить на Ваши вопросы. Если временные рамки не позволят охватить полностью весь их спектр, буду рад ответить на них по приведённым контактам!