



DevCon School

Blockchain

#msblockchain



Распределенная разработка распределенных систем

Дмитрий Булычков
Менеджер проектов
ЦТИ Сбербанк



Задача 1 – Познакомиться со взглядом Сбербанка на блокчейн

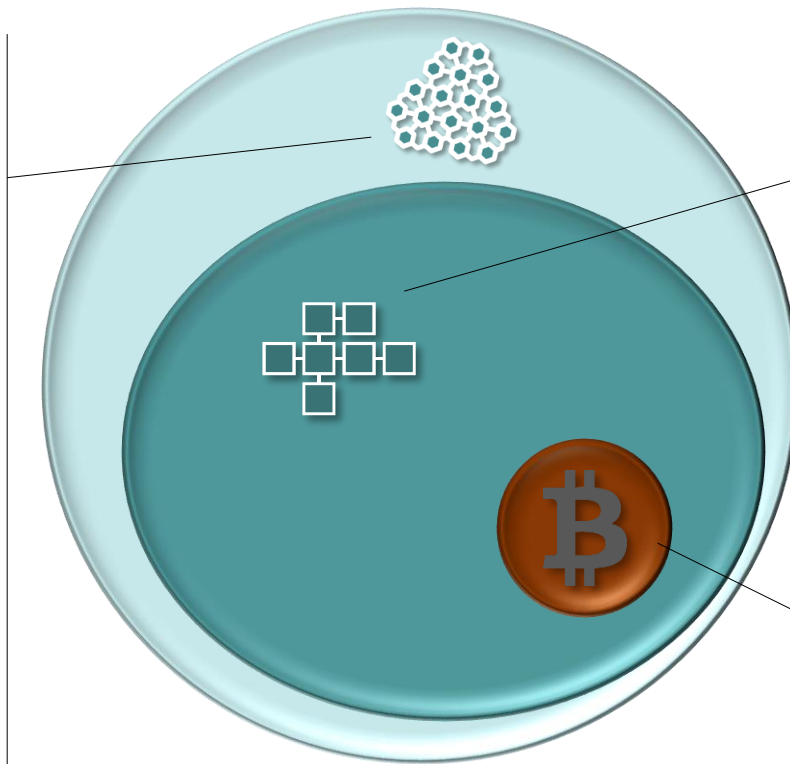
Задача 2 – Познакомиться с опытом блокчейн проектов Сбербанка

Задача 3 – Обсудить подходы к распределенной разработке
распределенных систем

Распределенные системы

Технология **обмена данными** между участниками, в которой:

- Каждый участник обладает полноценной копией реестра – т.е. Данные **распределены**
- Данные всех участников **полностью идентичны**
- **Синхронизация данных** всех участников происходит **автоматически на основе протокола** достижения распределенного консенсуса, а не за счет действий «центрального контрагента» (посредника)
- Каждый участник взаимодействия имеет **доступ к полной истории транзакций** – реестру истории взаимодействия



Блокчейн

Система (сеть) распределенно-согласуемых реестров, в которой данные о совершенных транзакциях структурируются в виде цепи (последовательности) связанных блоков транзакций

Биткойн

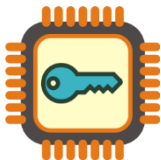
Пример цифровой валюты, которая реализована на технологии блокчейн(в виде открытой сети), в которой данные структурируются в виде цепочки блоков, и в которой применяется Proof-of-Work как подход для достижения распределенного консенсуса





Децентрализованная - отсутствует единый центр контроля и эмиссии.

Распределенная — данные и их обработка распределены по разным вычислительным узлам системы



Доверие — участники доверяют алгоритмам и проверяют ими информацию других участников, неизменность информации

Публичность — доступность всей информации всем участникам сети



Публичные



Bitcoin



Litecoin

- Открытая
- Псевдо-анонимная
- Транзакционная
- Любой может быть майнером
- Конкурентный майнинг
- Отсутствие регулятора

Регулируемые

- Открытые данные
- Полная идентификация
- Универсальная
- Закрытый перечень майнеров
- Комбинированный майнинг,
- Есть регулятор

Частные



hyperledger

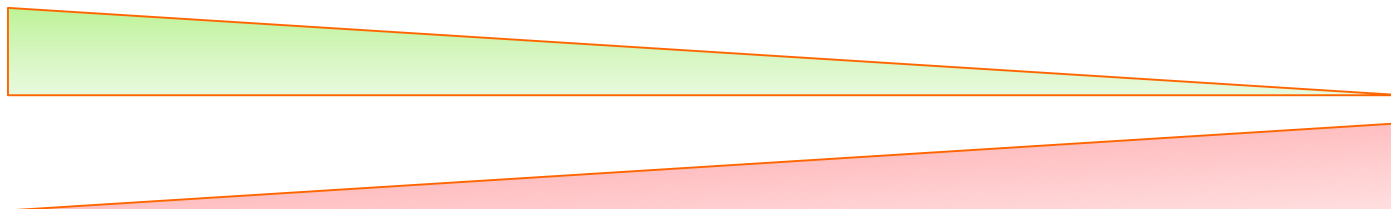


ripple

- Закрытая
- Полная идентификация
- Управление активами
- Закрытый перечень майнеров
- Ротационный майнинг
- Есть регулятор

Открытость

Централизация





Рост скорости проведения транзакций и расчетов за счет исключения промежуточных звеньев



Снижение стоимости транзакций за счет неопосредованного взаимодействия и снижения кредитного риска при расчетах в системе



Прозрачность взаимодействия из-за открытой истории транзакций и возможности отслеживания реального наличия активов



Безопасность за счет продвинутых методов криптографии и электронной подписи (включая множественную подпись), а также распределенное хранение



Устойчивость системы к локальным сбоям за счет распределенного характера процессинга и хранения



Доступность для пользователей за счет распределенности вычислений



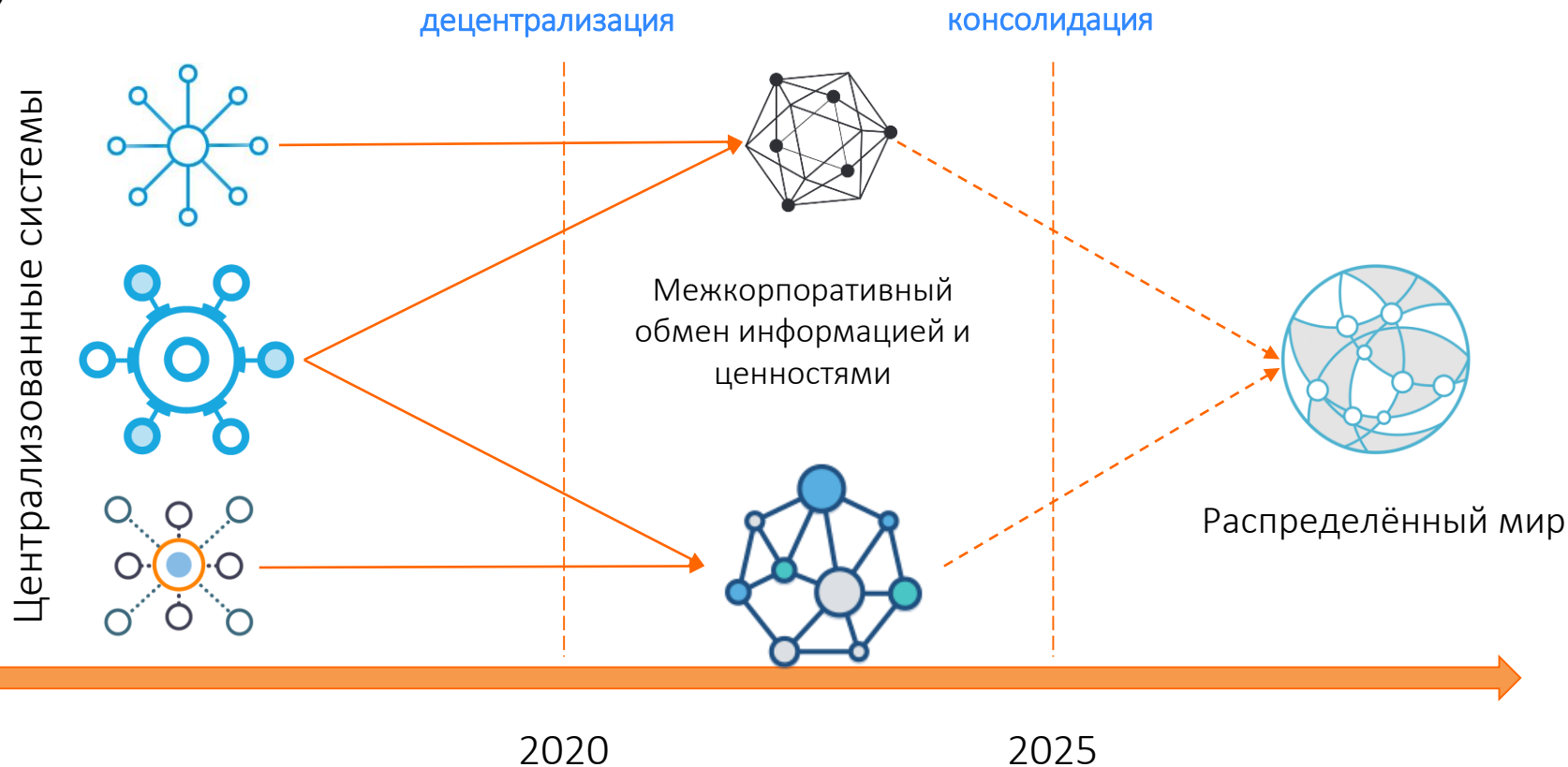
Возможность программировать систему (цифровые или **смарт контракты**)



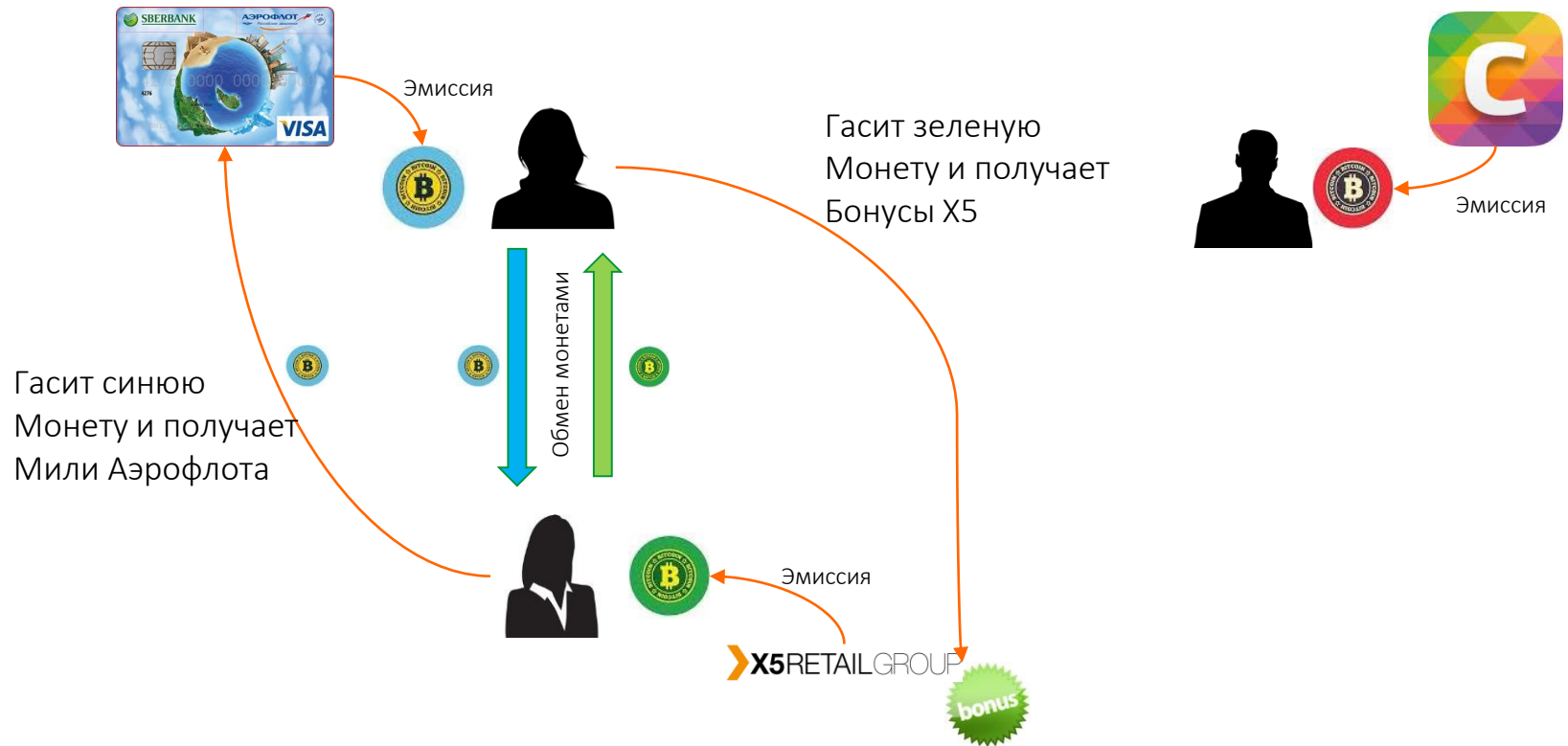
Универсальность системы – возможность использования одной инфраструктуры сети для операций с различными типами активов



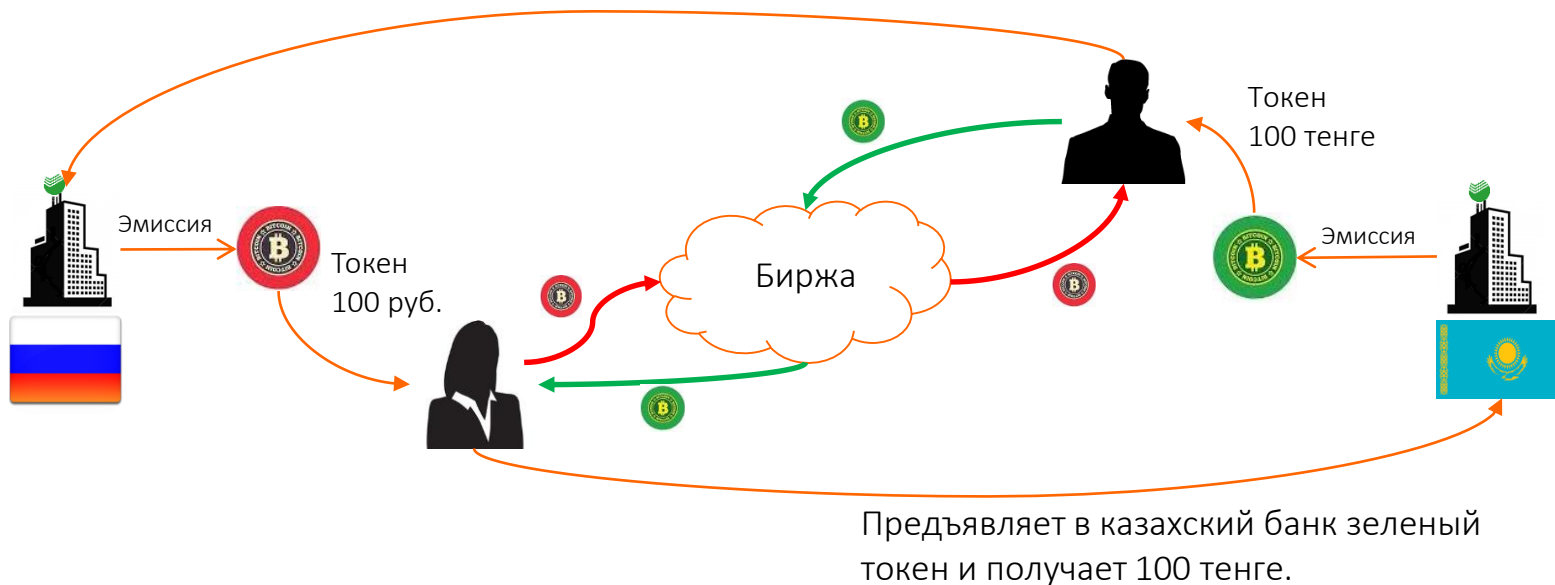
Эволюция в блокчейн



Мы попробовали

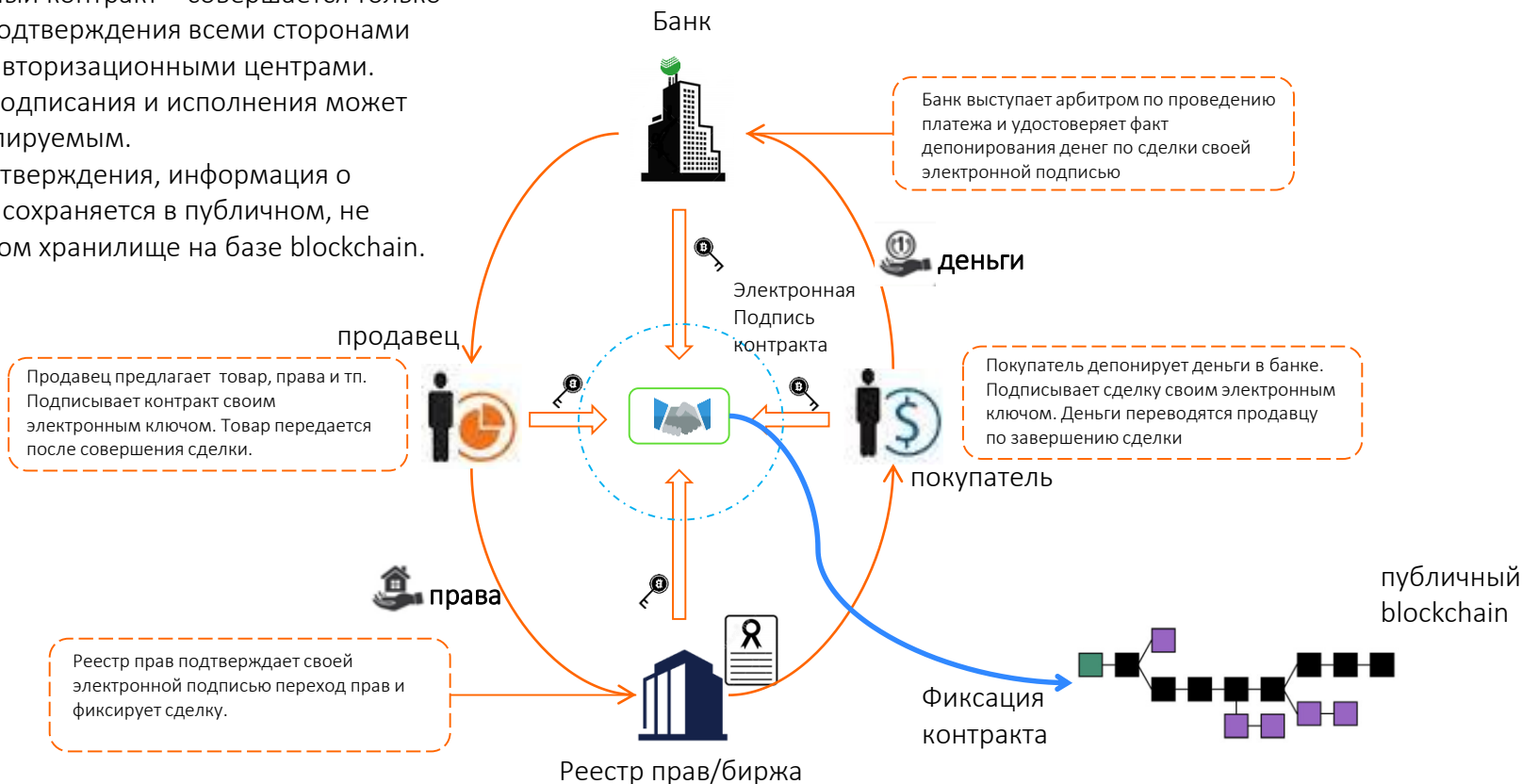


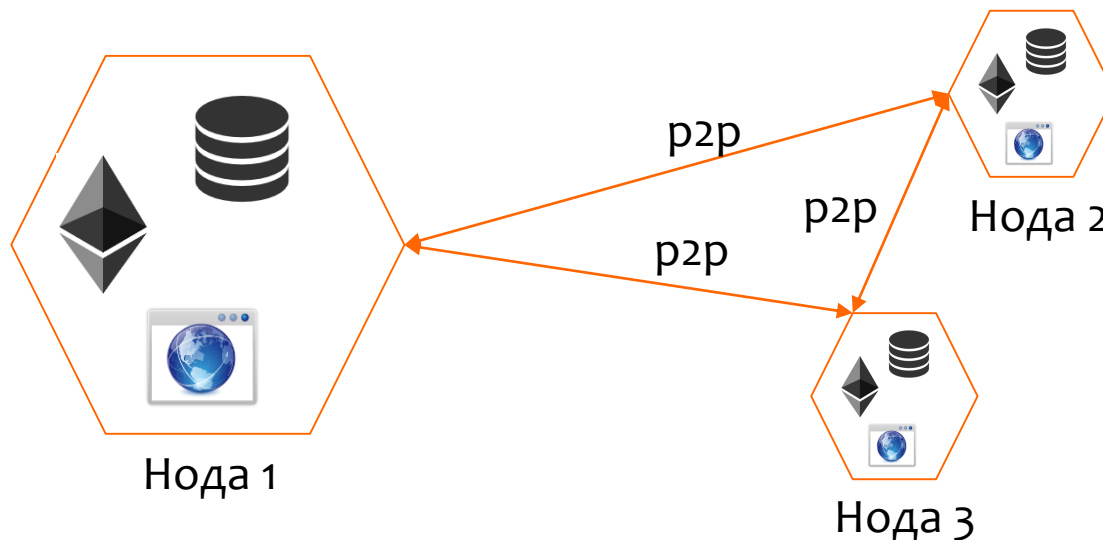
Предъявляет в российский банк красный
токен и получает 100 рублей.



При проведении обмена денежные средства не пересекают границу. Происходит только обмен «цветными монетами» (токенами). Работа и курсовая политика «Биржи» - отдельный бизнес

Электронный контракт – совершается только в случае подтверждения всеми сторонами сделки и авторизационными центрами. Порядок подписания и исполнения может быть регулируемым. После подтверждения, информация о контракте сохраняется в публичном, не изменяемом хранилище на базе blockchain.





- Система состоит из независимых нод
- Каждая нода обладает полной копией данных и синхронизирует их с системой стандартными p2p средствами базы данных и Ethereum
- Оператор работает со своей локальной нодой через web интерфейс (node.js/ReactJS)
- Документы сохраняются в локальном экземпляре распределенной БД и реплицируются стандартными механизмами
- Операции с документами отмечаются в блокчейне Ethereum и данные об операциях реплицируются стандартными средствами Ethereum по все сети
- Smart-contracts Ethereum'a ведут мониторинг операций с документами и дают обратную связь оператору (web, email)



Особенности системы

- Отсутствует централизованное хранилище документов
- Версионность и совместная работы (редактирование, обсуждение, сообщения, чаты)
- Последняя версия «правды» у всех участников
- Система всегда доступна для работы, документы хранятся локально на рабочих станциях
- Документ доступен только участникам работы над ним. Встроенное шифрование и электронная подпись.
- Автоматическая синхронизация, восстановление процессов и тп, после сбоев и разрывов соединения
- Устойчивость к потере информации за счет ее дублирования на разных узлах
- Модульная система (конструктор Lego), легкое добавление функций без нарушения существующих, гибкое конфигурирование и подключение новых функций
- Автоматический аудит и арбитраж, ведение не изменяемых журналов работы с системой
- Система голосования/согласования



Текущее состояние :

- Создан рабочий прототип реализующий распределенный документооборот
- Запущен пилот по использованию системы между Сбербанком, ФАС, Аэрофлот, Русский Уголь и несколькими заинтересованными участниками

Развитие:

- Адаптация различных систем хранения – Git, Hadoop, IPFS
- Создание «движка» по подключению модулей (BPM, work flow и тд)
- Создание системы внутреннего аудита и арбитража
- Реализация согласований и голосований
- Подключение сертифицированной криптографии (для целей использования в государственном документообороте)
- Пилотирование на регионах Москва, С.Петербург, Татарстан



Дальнейшее развитие:

- Decentralized Autonomous Organization (DAO)
- Автоматизация и роботизация процессов на базе smart-contracts
- Реализация в системе элементов Искусственного Интеллекта
- Переход к парадигме «Бирюзовой организации»





Межбанковская ассоциация

Департамент финансовых технологий, проектов
и организации процессов ЦБ РФ





Будущее

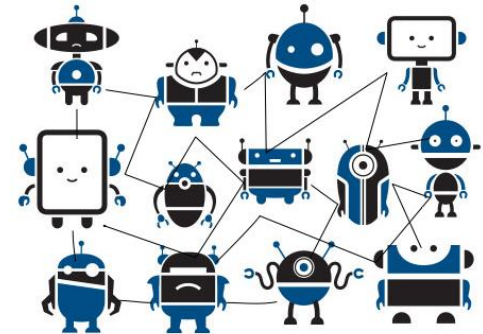
1980-е



2010-е



2050-е



Подходы к распределённой разработке

Применение подходов Open Source к корпоративной разработке

Open source style development

Как это работает у нас на практике

Спасибо

Центр технологических инноваций
Декабрь 2016
Булычков Дмитрий
dabulychkov2@sberbank.ru