



Распределенный реестр и смарт-контракты в бизнесе

DLT vs. Blockchain

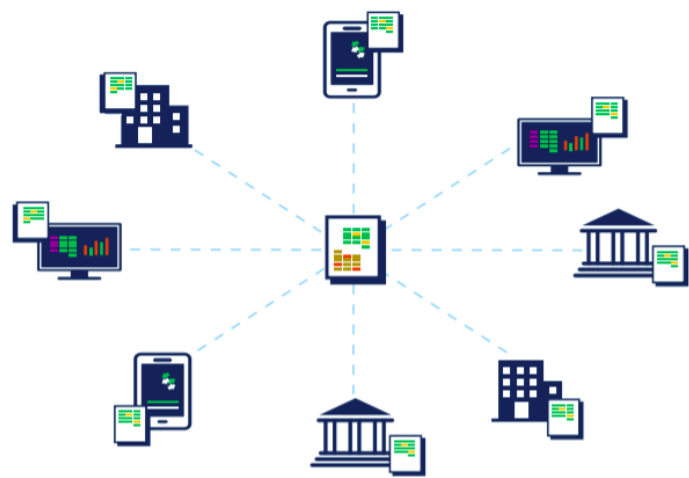


Распределенный реестр		Блокчейн
закрытый	Доступ к сети	открытый
разграничен	Доступ к данным	все видят всё
PoA, PoET	Консенсус	PoW/PoS («51%»)
не ограничена	Производительность	ограничена
участие в сделке	Мотивация	майнинг / комиссии

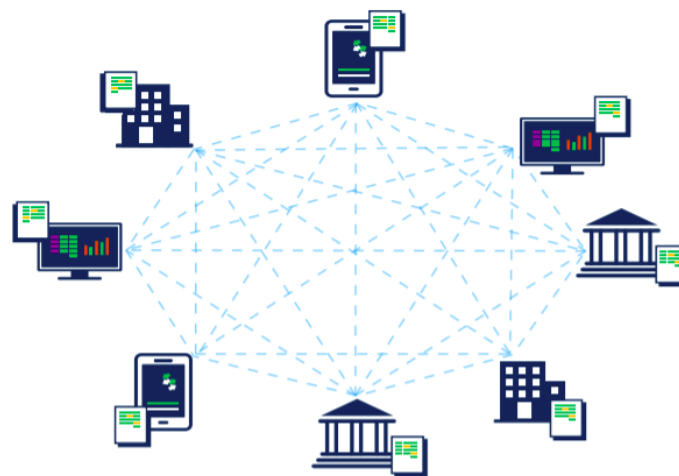
В чем смысл?



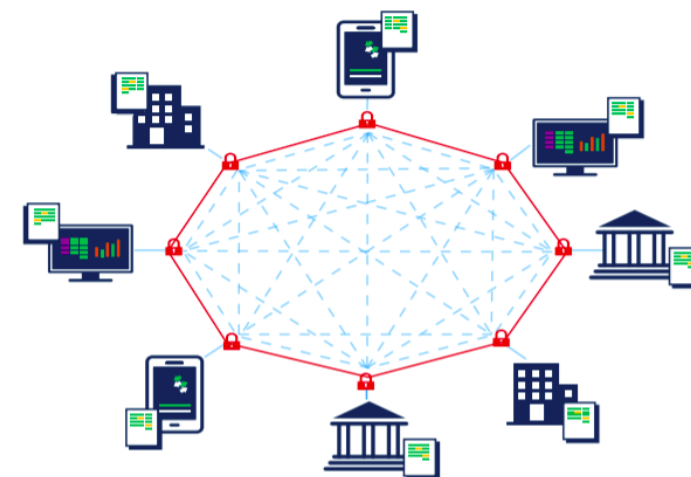
Традиционная архитектура



Открытый блокчейн



Распределенный реестр



Логическая архитектура корпоративной DLT-сети



В отличие от «публичных блокчейнов», в корпоративных сетях участники имеют доступ к транзакциям и данным в рамках изолированных каналов.

Конфигурация каналов выстраивается в соответствии с потребностями участников.

Узел каждой организации может участвовать в нескольких каналах одновременно.



Ledger: world state

Содержит текущие значения данных, полученные из утвержденных транзакций.



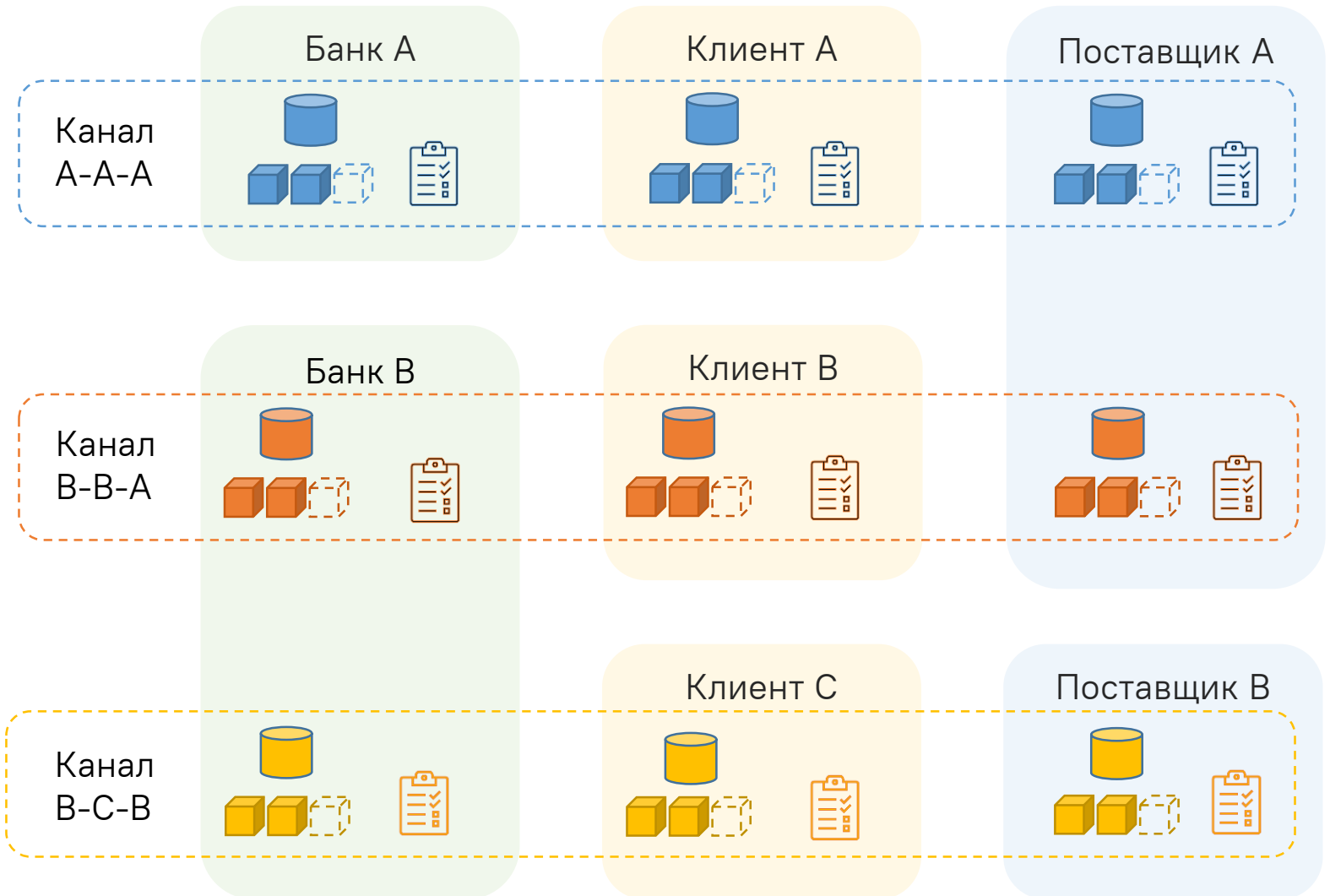
Ledger: блокчейн

Летопись транзакций из взаимосвязанных блоков, где каждый блок состоит из последовательности транзакций, изменяющих world state.



Смарт-контракты

Определяют транзакционную логику (бизнес-процессы) и взаимодействуют с блокчейном и world state с одной стороны, и с клиентскими приложениями и сервисами. Смарт-контракты могут одновременно работать в нескольких каналах, в то время как блокчейн и world state уникальны для каждого канала.



Сетевая архитектура корпоративной DLT-сети



Сеть формируется из сегментов организаций.

Каждый сегмент может состоять из:

1. **Peers** — узлы для обработки транзакций
2. **Orderers** — узлы для упорядочивания транзакций в блоках

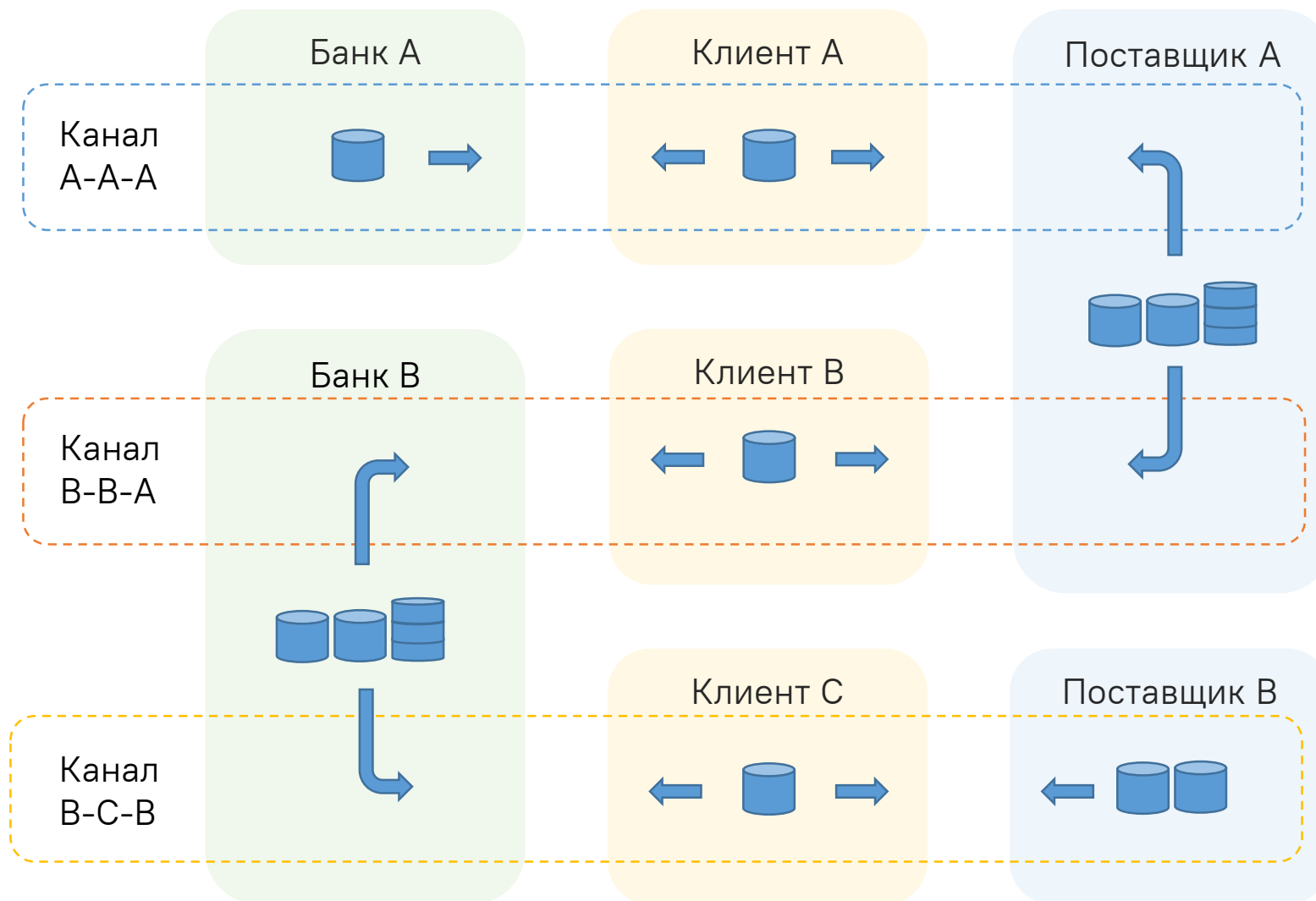
Конфигурация каждого сегмента зависит от:

1. нагрузки на организацию
2. роли организации
3. политик канала/сети

Для решения типовых задач, как правило, большинству компаний достаточно двух веб-серверов среднего уровня в роли peers.

Для высоконагруженных крупных компаний и банков может быть развернут кластер, включающий дополнительные СХД и HSM.

Взаимодействие между сегментами организаций защищено программным TLS.



Архитектура корпоративного сегмента



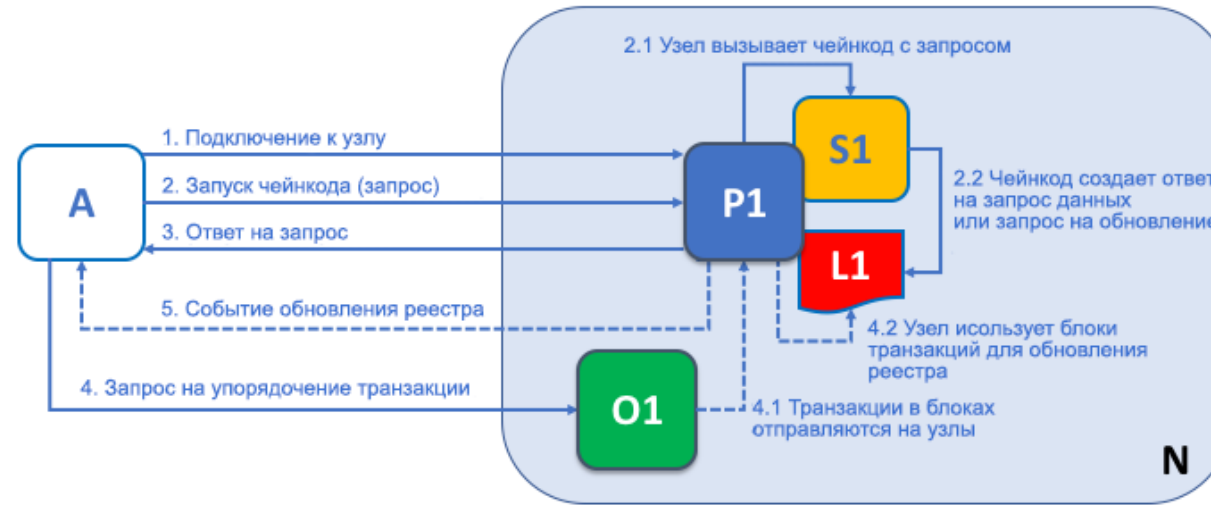
Peers совместно с *orderers* обеспечивают синхронизацию данных реестра для каждого узла в сети.

Работа с узлом осуществляется из корпоративной системы или веб-сервиса, которые обращаются к своему узлу и вызывают нужный чейнкод (смарт-контракт).

Чейнкод — это программная реализация смарт-контракта на Java, Go или Node.js.

Чейнкод выполняется на узлах контрагентов и создает согласованный ответ на запрос данных или запрос на обновление реестра.

В итоге приложение направляет запрос на внесение транзакции ордереру, который валидирует транзакцию с задействованными в процессе узлами, упорядочивает и вносит в блокчейн.



Другими словами, на каждом узле у нас есть:

1. Распределенная база данных, состояние которой согласовано с другими участниками канала.
2. Сервер приложений, который обеспечивает исполнение смарт-контрактов.
3. TLS-сервер, который обеспечивает защиту каналов передачи данных.

Авторизация участников и конфиденциальность данных



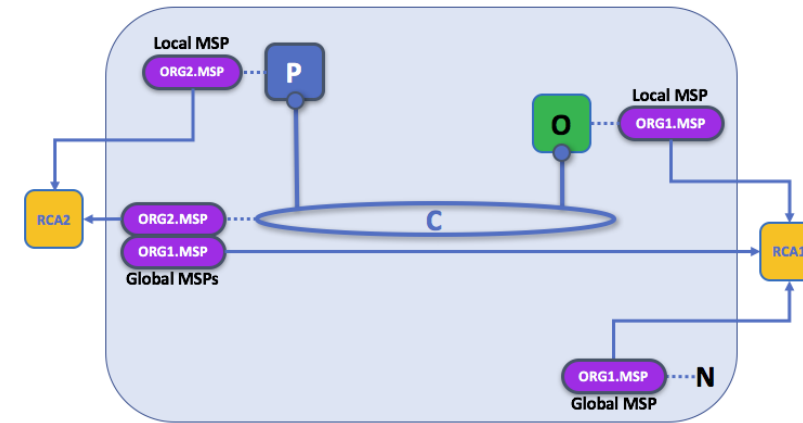
Участниками блокчейн-сети являются пиры, ordering-службы, клиентские приложения, администраторы и многие другие.

Каждый участник имеет набор цифровых identity в виде цифровых сертификатов X.509, которые выдаются удостоверяющими центрами.

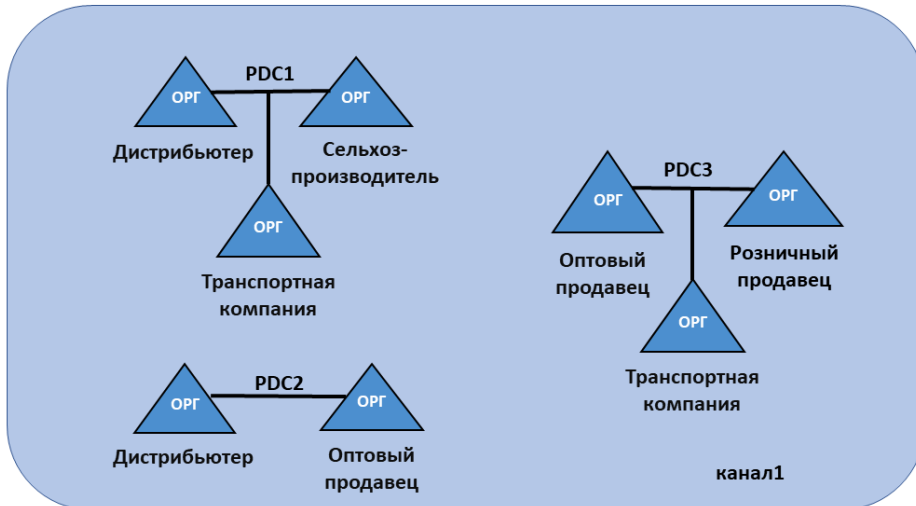
Управление правами доступа участников на уровне узлов, каналов и всей сети осуществляется сервисами MSP, конфигурация которых зависит от роли отдельной организации и общей топологии сети.

В нашей версии Fabric мы используем ГОСТ, что обеспечивает:

1. интеграцию с отечественной инфраструктурой открытых ключей;
2. юридическую значимость транзакций;
3. соответствие требованиям регуляторов (ПКЗ-2005 ФСБ РФ, 757-П ЦБ РФ).



N	Blockchain Network
C	Channel
MSP	Membership Services Provider
P	Peer
O	Orderer
CA	Certificate Authority



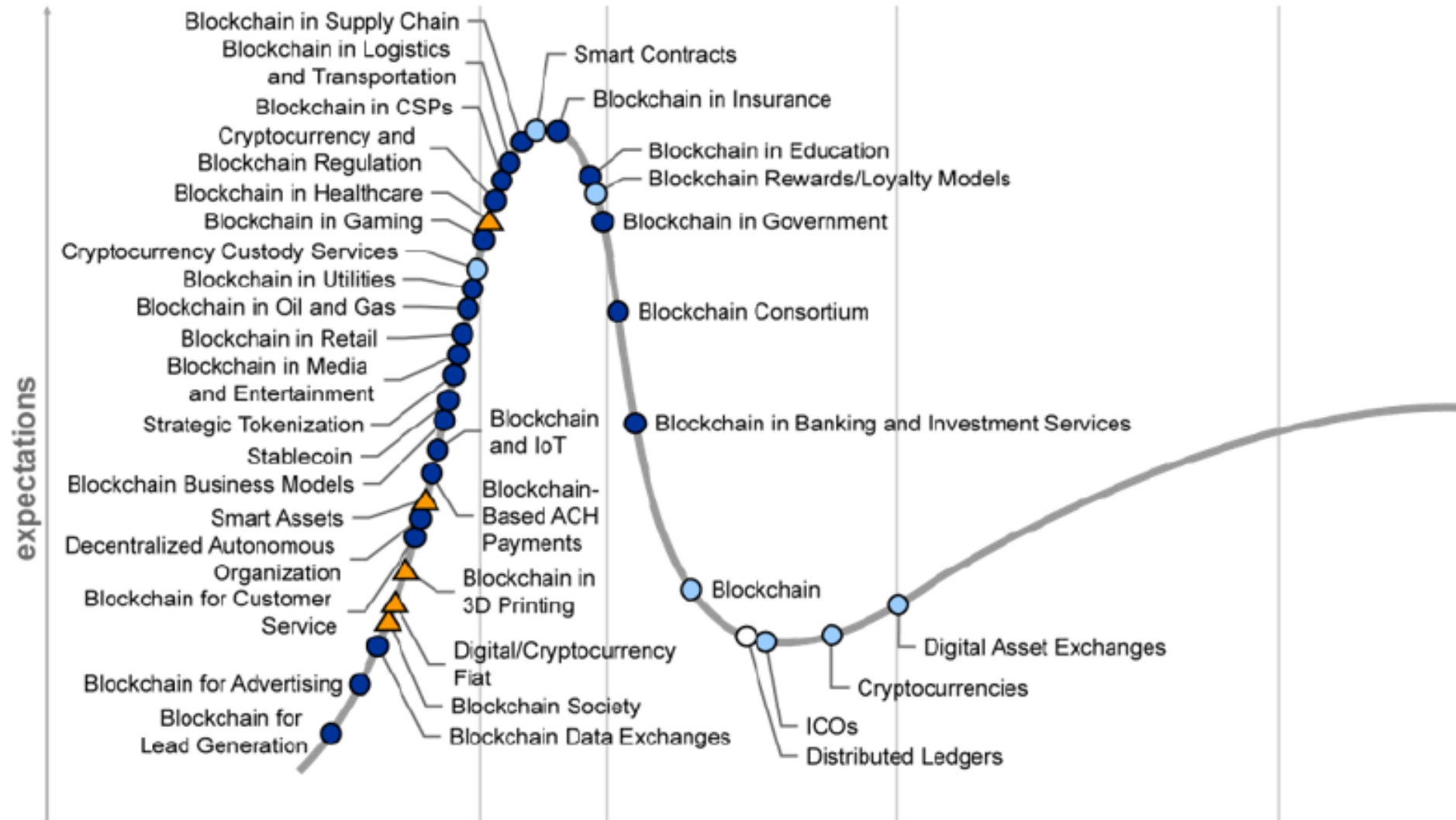
Коллекции конфиденциальных данных

Кроме изоляции данных средствами каналов, для разграничения доступа к данным между подмножеством организаций в отдельном канале применяются коллекции конфиденциальных данных (PDC, private data collection).

Участники коллекции могут дать доступ к данным другим участникам, если у них возникнут разногласия или если они решат поделиться данными с третьей стороной, которая может вычислить хеш конфиденциальных данных и проверить, сходится ли он с состоянием реестра канала, и если да, то это будет служить доказательством существования состояния канала в определенный момент времени.

Применение PDC позволяет минимизировать накладные расходы на управление данными в сети.

Gartner's Hype Cycle for Blockchain Business, 2019



Области применения



- | | | | | | |
|---|-------------------|---|-----------|---|-----------------|
| 1 | Ценные бумаги | 4 | Логистика | 7 | Агробизнес |
| 2 | Платежные системы | 5 | Транспорт | 8 | Здравоохранение |
| 3 | Финансовые услуги | 6 | ESG | 9 | АСУ ТП / IoT |

Выгоды применения



Быстрее: операции в режиме реального времени

Дешевле: снижение транзакционных издержек

Выгоднее: новые финансовые инструменты

Цифровые права

1. Эмиссионные ценные бумаги
2. Денежные требования
3. Участие в капитале

Что это дает?

1. Ускорение оборота финансовых инструментов
(облигации, векселя и т.д.)
2. Токенизация активов
(сырье, товары, услуги)
3. Онлайн-управление бизнесом

Виды токенизированных активов



Токен, обеспеченный сырьевым товаром

- **Торговый:** токенизация торговых контрактов
- **Инвестиционный:** токенизация актива, ценного для инвесторов

Токен, обеспеченный правом требования

услуги/ товара / скидки

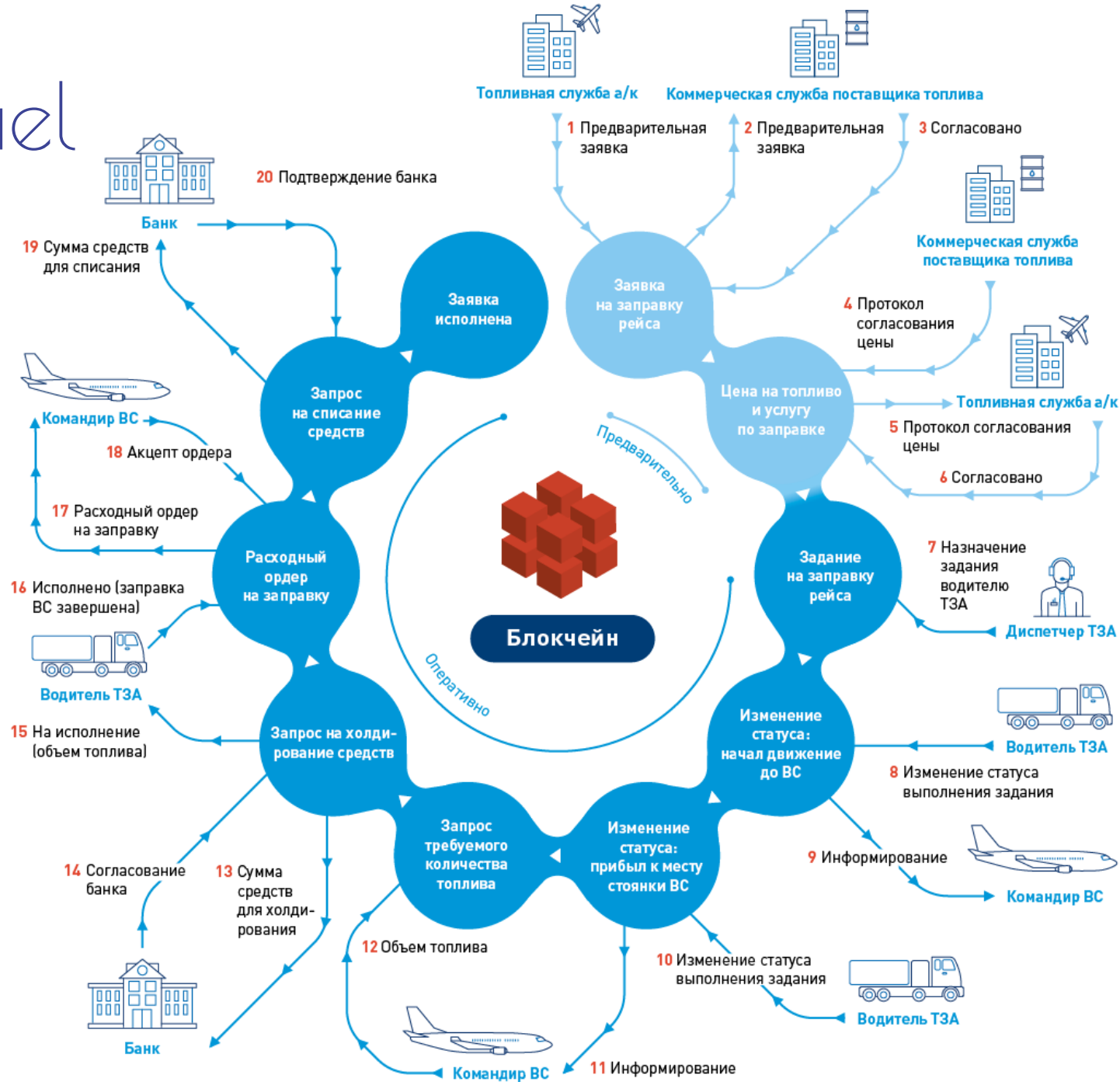
Токен, обеспеченный финансовым инструментом

акции, облигации и т.д.

Опыт внедрения



SmartFuel



Подготовка к заправке



1. Создание заявки со стороны авиакомпании

Ключевые параметры:

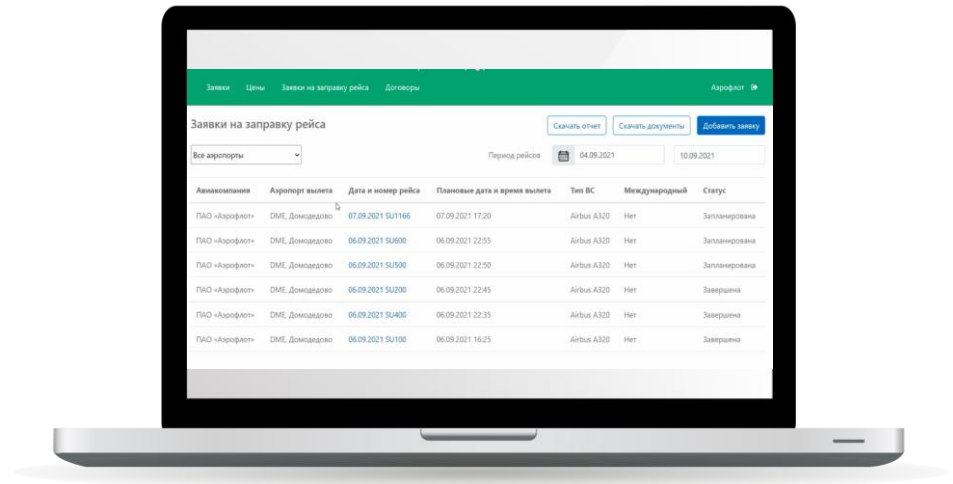
- Аэропорт вылета
- Аэропорт назначения
- Номер борта
- Плановое количество топлива к заправке
- Командир ВС, назначенный на рейс

2. Запрос топлива КВС

Командир ВС запрашивает количество топлива к заправке

3. Авансирование заправки

- расчет стоимости
- формирование платежного поручения
- выполнение платежа



Выполнение заправки



4. Заправка

- заправка
- формирование расходного ордера ТЗК
- согласование расходного ордера АК

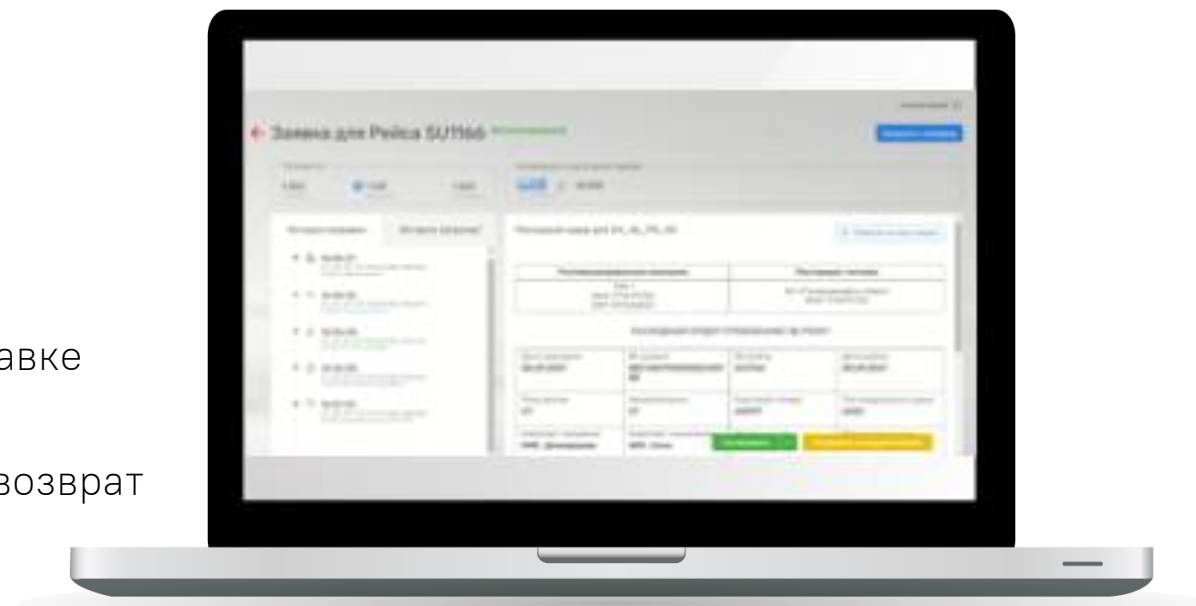
5. Автоматические взаиморасчеты

Командир ВС запрашивает количество топлива к заправке

- расчет фактической стоимости
- формирование платежного поручения на доплату/возврат
- выполнение/планирование платежа

5. Формирование отчетности

- Платежи
- Расходные ордера
- Расчет стоимости запросов КВС
- Расчет фактической стоимости



Системный эффект

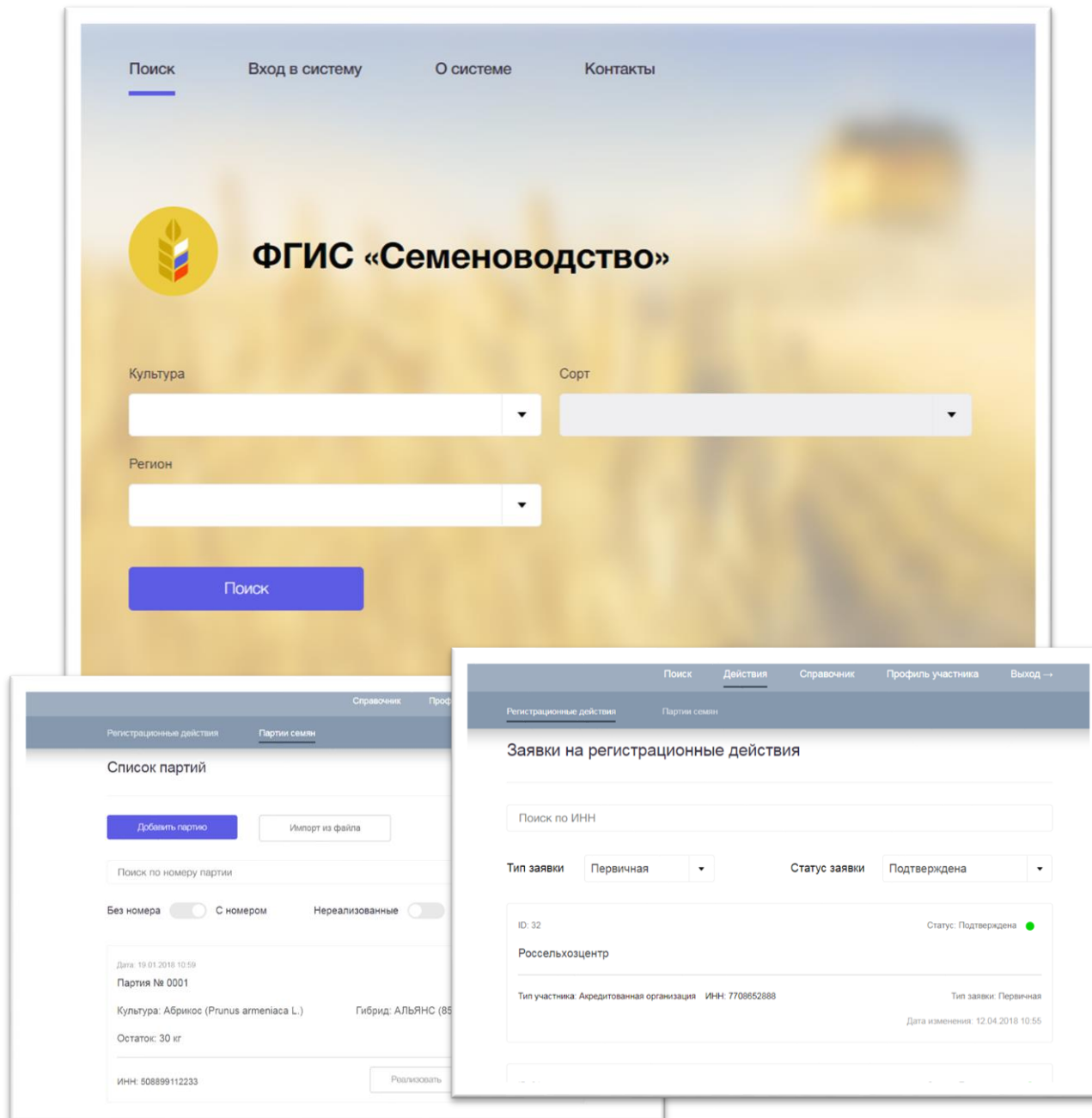
1. Переход на оплату заправки в реальном времени:
 - минимизация финансовых рисков для топливной компании
 - нет необходимости предоплаты для клиента
2. Максимальная утилизация ресурсов топливозаправочных комплексов за счет онлайн-синхронизации данных между компаниями
3. Оптимизация ФОТ топливозаправочных компаний на 9%

[Подробнее о проекте на TADVAISER](#)

Метрика	Было	Стало
Время организации заправки при изменении расписания	до 25 минут	1 – 3 минуты
Ручные операции по оформлению документов	> 50 000	0
Время оплаты	от 3 дней	11 секунд
Время оформления документов	до 7 дней	1 секунда

ФГИС «Единая система управления семеноводством»

- регистрация партий посевных материалов
- прослеживание партий на рынке
- информирование конечных потребителей



Поиск Вход в систему О системе Контакты

 **ФГИС «Семеноводство»**

Культура Сорт

Регион

Поиск

Справочник Профиль участника Выход

Регистрационные действия Партии семян

Список партий

Добавить партию Импортировать из файла

Поиск по номеру партии

Без номера С номером Нереализованные

Дата: 19.01.2018 10:59
Партия № 0001
Культура: Абрикос (Prunus armeniaca L.) Гибрид: АЛЬЯНС (85)
Остаток: 30 кг
ИНН: 508899112233

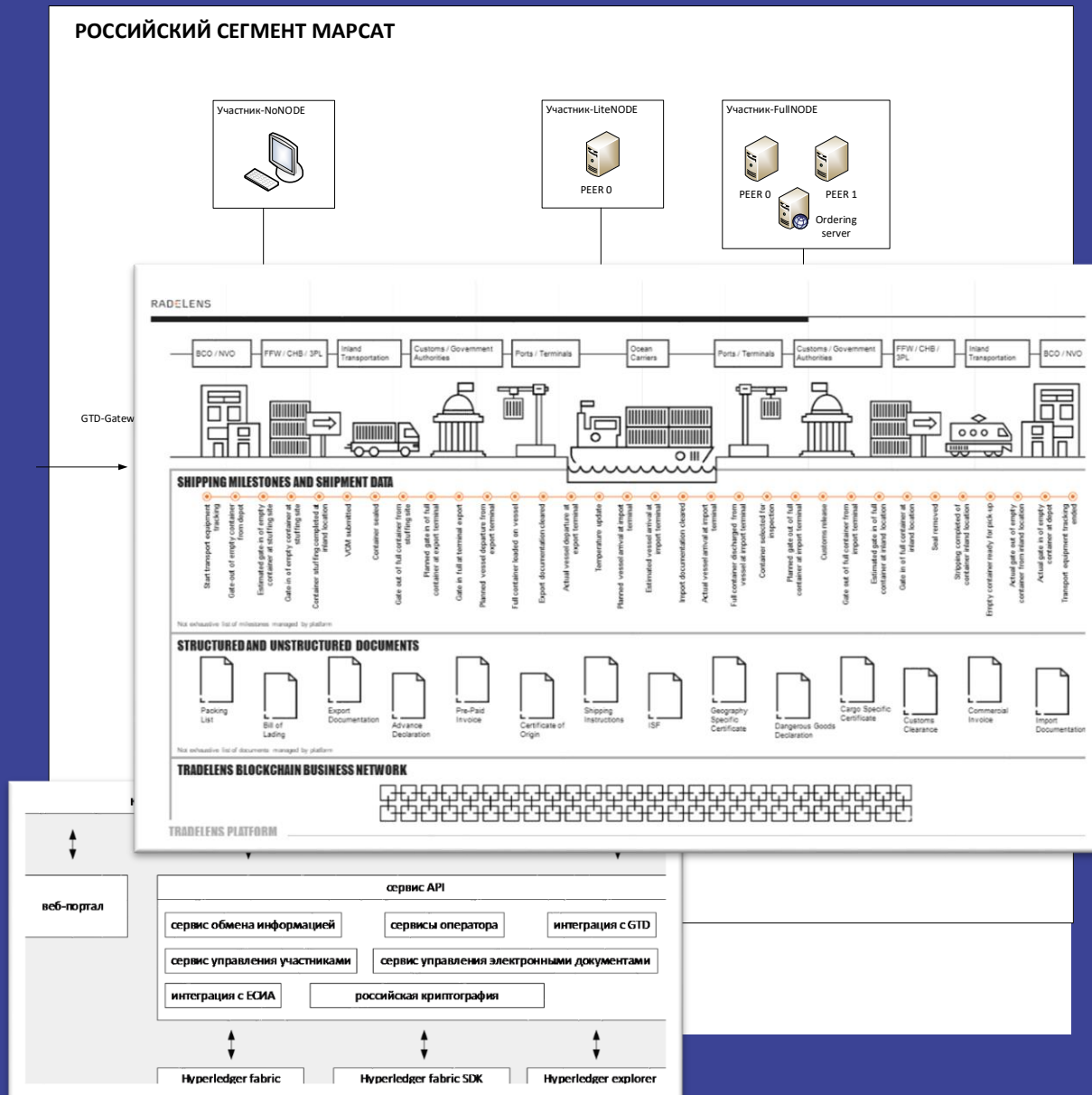
Заявки на регистрационные действия

Поиск по ИНН

Тип заявки: Первичная Статус заявки: Подтверждена

ID: 32 Статус: Подтверждена
Россельхозцентр
Тип участника: Аккредитованная организация ИНН: 7709652888
Тип заявки: Первичная
Дата изменения: 12.04.2018 10:55

РОССИЙСКИЙ СЕГМЕНТ MAPCAT



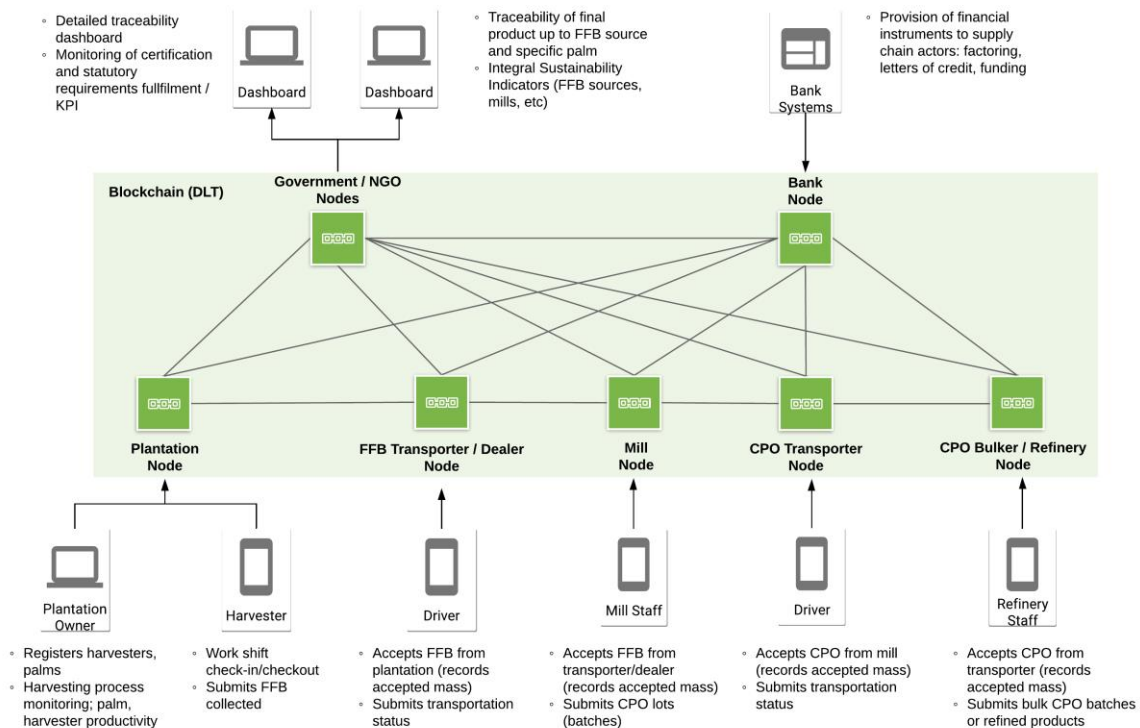
Платформа Tradelens: российский сегмент

Крупнейшая в мире коммерческая сеть по управлению контейнерными перевозками.

В 2018 году по заказу ФГУП «Морсвязьспутник» мы разработали концепцию российского сегмента сети.

Концепция обеспечивает участие российских организаций в глобальном проекте с учетом требований к информационной и экономической безопасности. Согласована заинтересованными ведомствами и утверждена Правительством РФ.

В 2019 году нами разработан комплект проектно-технической документации для пилотного проекта на базе большого порта Санкт-Петербурга и технический проект российского сегмента.



Bloombloc

прослеживание происхождения масла – от плантаций до потребителей

контроль

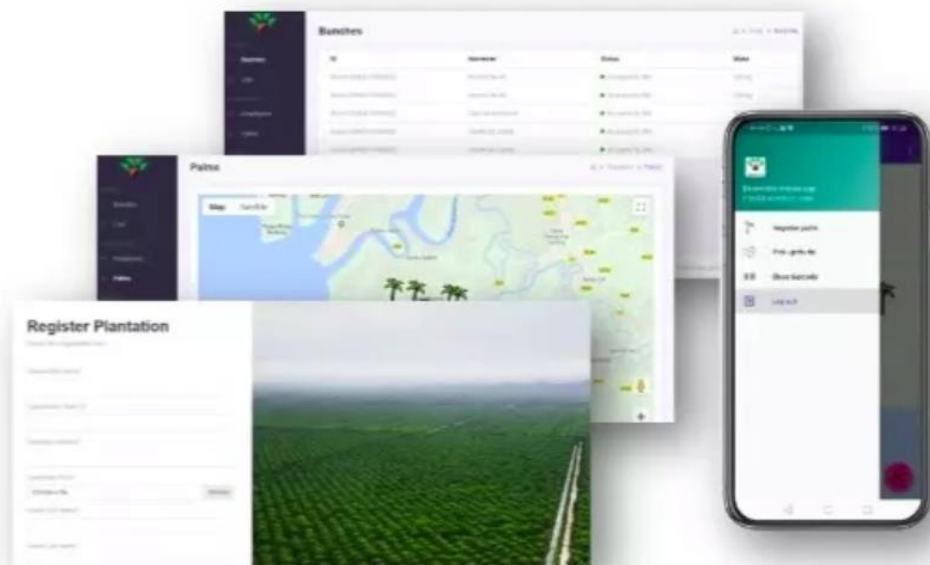
сбора пальмовых фруктов

персонала

оборудования

условий транспортировки

для выполнения требований по сертификации



Типовые проблемы при внедрении



- внедрение в контуре одной организации
- попытки внедрения криптовалютных платформ
- несертифицируемая криптография
- цифровой разрыв между участниками

Хауберк

корпоративная блокчейн-платформа

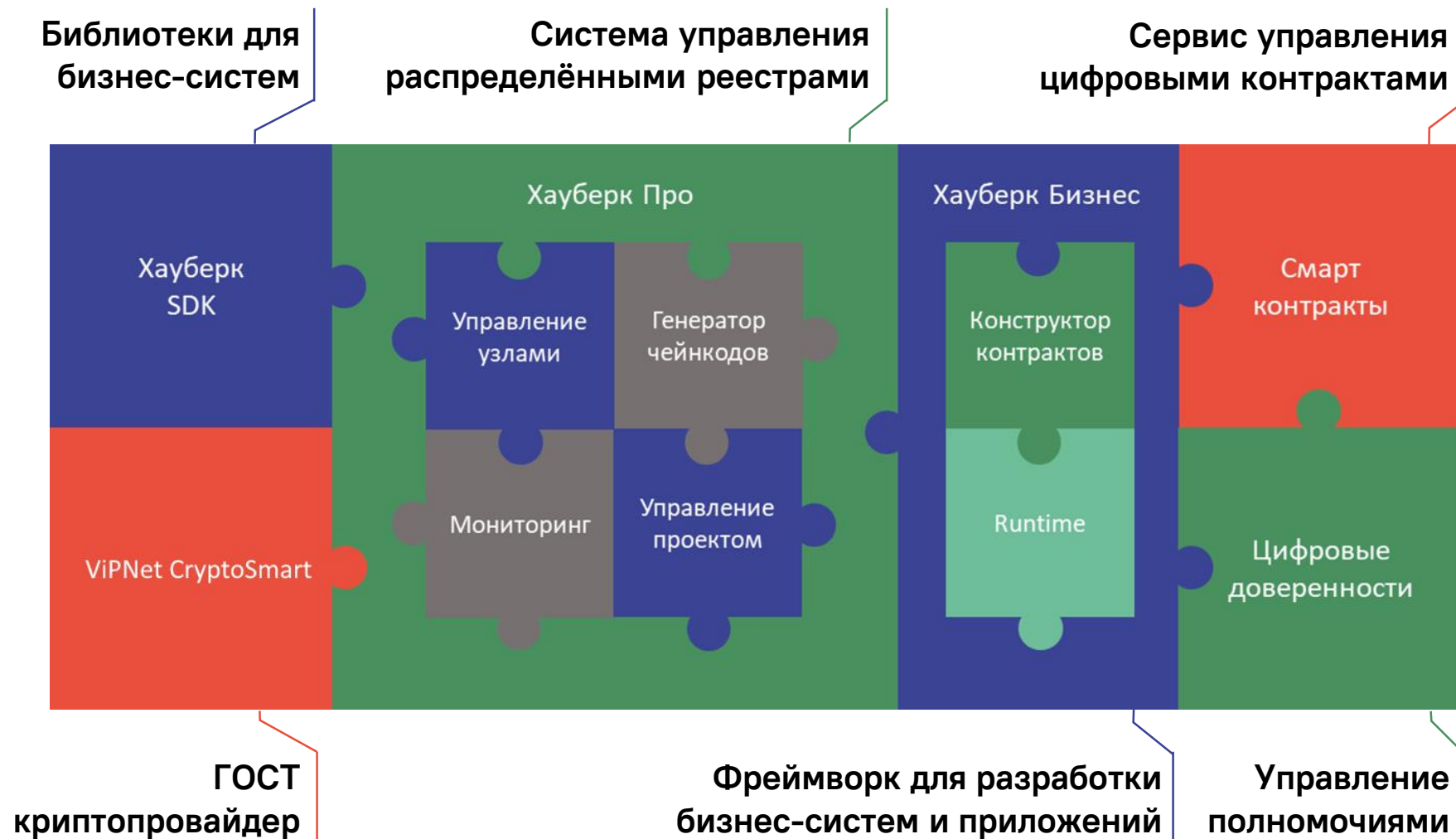


Зачем?

- безопасное прямое взаимодействие контрагентов в реальном времени

Преимущества

- низкий порог входа и TCO для бизнеса
- адаптирована для России/ЕАЭС
- совместима с платформами SAP/IBM/Oracle



Hyperledger Fabric

базовая технологическая платформа



Основные преимущества

- открытый исходный код (Linux Foundation)
- корпоративные стандарты безопасности
- развитая система управления доступом к данным
- модульная архитектура
- зрелая экосистема, наличие long-term support версий
- поддержка ключевых вендоров
- отсутствие криптовалют и майнинга

Проекты на Fabric

в России:

- Сбербанк
- ВТБ
- Альфа-Банк
- Московская биржа / НРД
- РЖД / Локотех
- Газпром нефть
- Минсельхоз РФ
- Минтранс РФ

ViPNet CryptoSmart

Специализированное СКЗИ для встраивания в криптосистемы на базе HLF 2 / Хауберк:

- защита конфиденциальных данных
- интеграция с отечественной PKI
- соответствие требованиям ПКЗ-2005

CryptoSmart находится на сертификации в ФСБ России на соответствие требованиям к СКЗИ и средствам ЭП класса КС2.



Хауберк Про

Система управления распределенными реестрами и смарт-контрактами



Zero-code

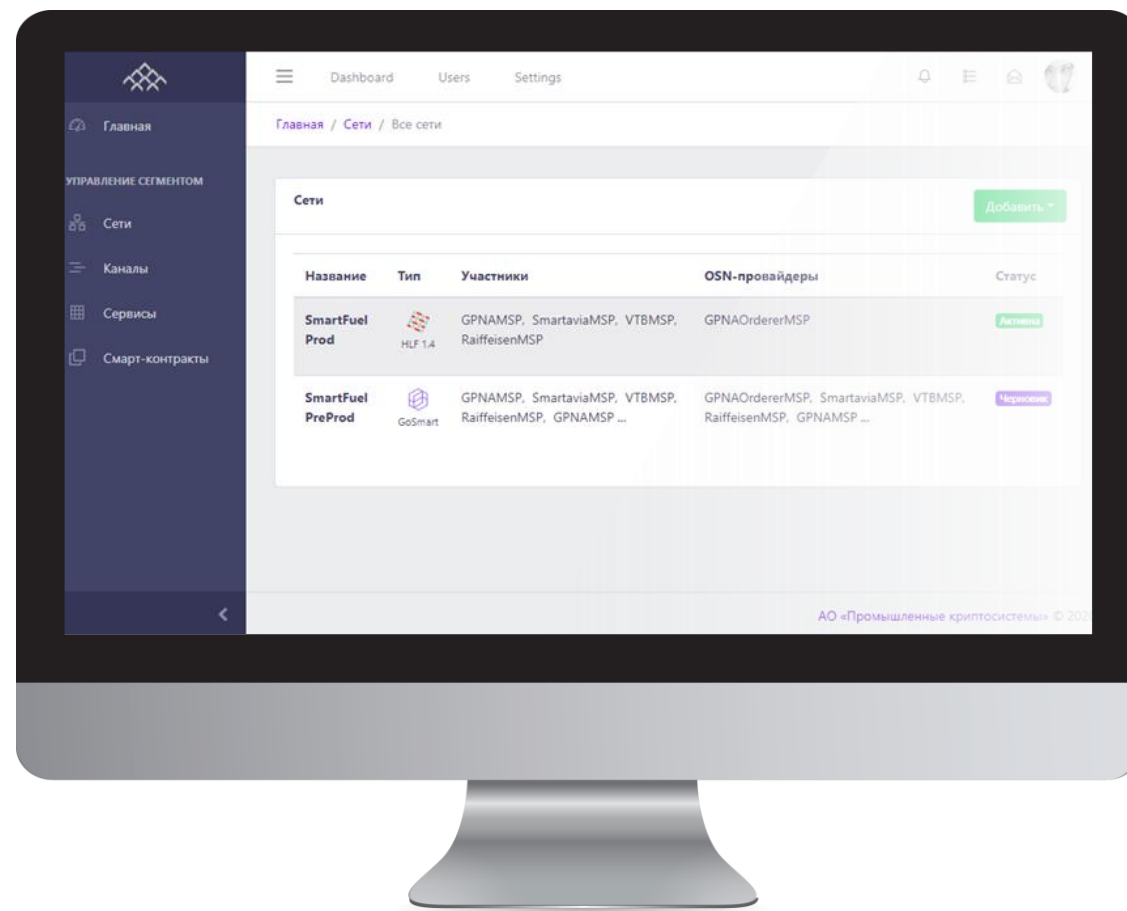
Управление реестрами в один клик для операторов сетей и бизнеса

Agile + CI/CD

Тиражирование смарт-контрактов между организациями

Smart generation

Генерация смарт-контрактов из UML/BPMN для бизнес-аналитиков и разработчиков



Для кого?

- Организаторы консорциумов, например операторы ЦФА-платформ
- Сервис-провайдеры (операторы обмена ЦФА, информационных сервисов и т.д.)
- Бизнес

Зачем?

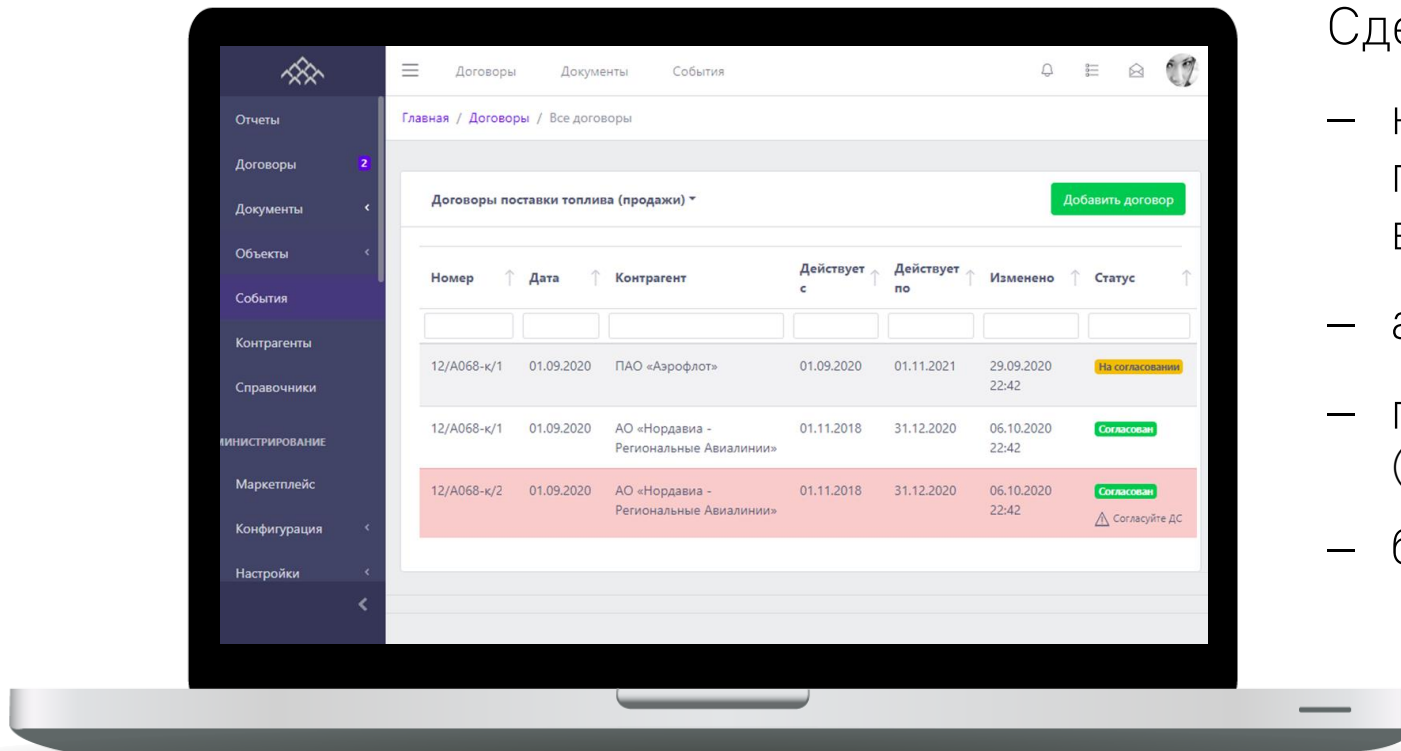
Снижение порога входа. Минимизация ТСО. Автоматизация рутинных операций.

Функциональные возможности

1. Управление сетями, каналами, участниками для оператора сети/консорциума
2. Управление сегментом сети для участника
3. Мониторинг доступности узлов
4. Управление развертыванием смарт-контрактов
5. Генерация чейнкода из диаграмм бизнес-процесса (UML/BPMN)

Хауберк Сمارт-Контракты

фреймворк управления цифровыми договорами

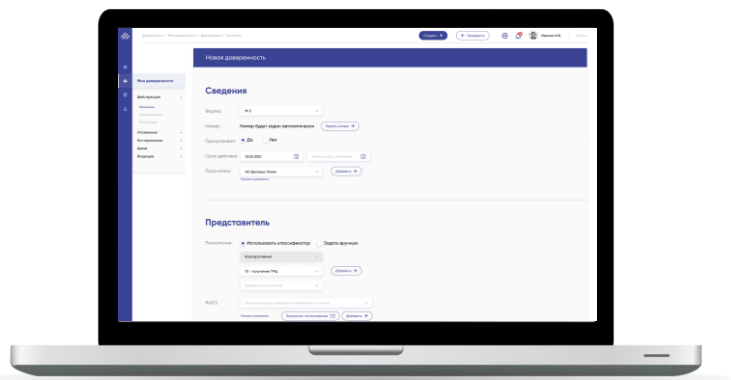


Сделки с контрагентами в онлайн:

- контроль исполнения сделок по цепочке поставщиков в режиме реального времени
- автоматизация рутинных операций
- переход на цифровой документооборот (машиночитаемые документы)
- без посредников и агрегаторов

Цифровые доверенности

сервис управления машиночитаемыми доверенностями



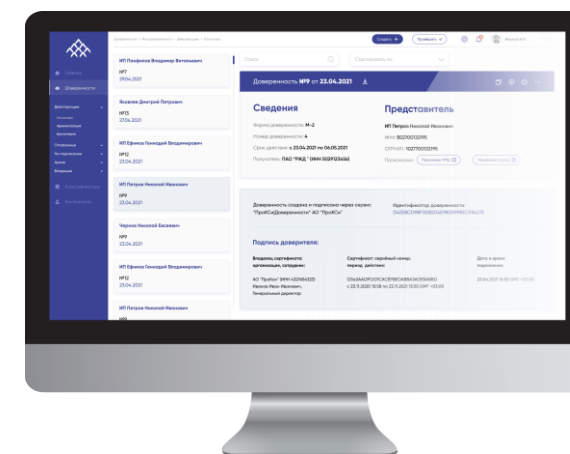
Сервис решает основные задачи управления МЧД для бизнеса в соответствии с новой редакцией 63-ФЗ.

Устраняет проблемы безопасной передачи и отзыва доверенностей между организациями, а также синхронизации классификаторов.

Позволяет интегрировать доверенности в бизнес-процессы, прежде всего в области логистики и B2B-продаж (передача ТМЦ).

Функциональные возможности

- управление доверенностями
 - создание (типовая, М2, ФНС...)
 - отзыв
 - раскрытие контрагентам
 - через реестр
 - XML-файл
 - API
- проверка доверенностей контрагентов
 - по паспорту
 - по токену
- интеграция с бизнес-системами через API/SDK



Следующие вебинары:

Система управления распределёнными реестрами и смарт-контрактами



05.10

Мастер-класс «Демонстрация
Hauberk Pro Admin»



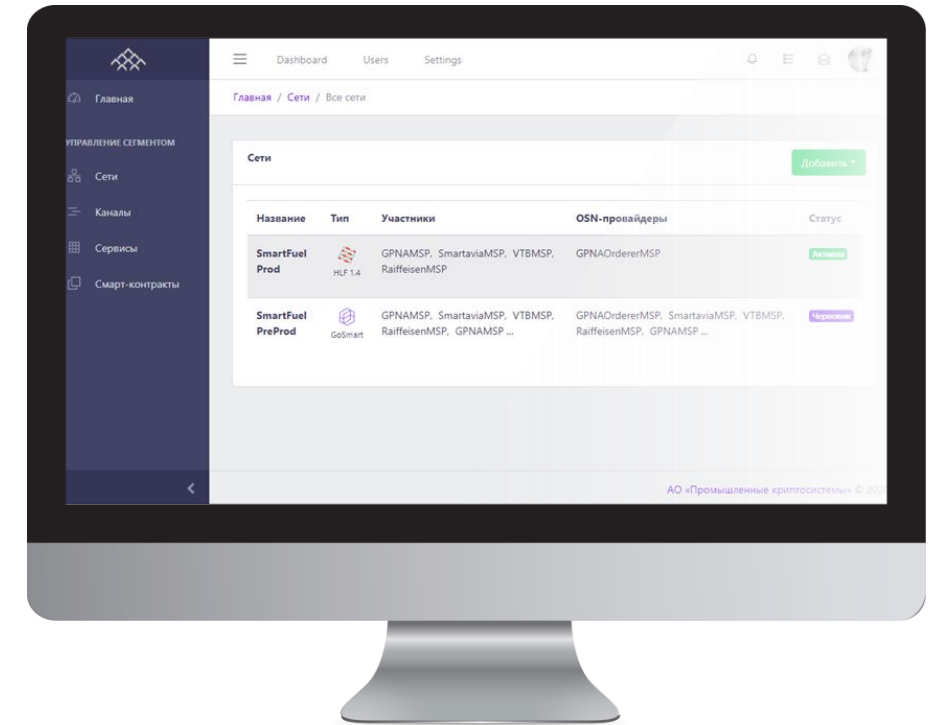
12.10

Мастер-класс «Демонстрация
Hauberk Pro Developer»



Для кого:

Менеджеры проектов, аналитики,
администраторы / девопсы





Спасибо!

Для обсуждения ваших задач и наших решений:

Михаил Чеканов
директор по развитию АО «ПроКСи»

+7 925 999 2414 / m@procsy.ru