

Лидирующий исследовательский центр в области систем распределенного реестра

УНИВЕРСИТЕТ ИННОПОЛИС



Основная цель ЛИЦ

Создание платформы InnoChain, которая:

- основана на полной формальной верификации — не требует «ручного» аудита
- отвечает отечественным требованиям безопасности
- включает специализированные языки программирования для верифицируемых смарт-контрактов
- интегрируется с другими блокчейн-решениями и отраслевыми информационными инфраструктурами

Срок проекта

с 1 января 2020 года
по 31 декабря 2021 года

Заказчик

Министерство цифрового развития,
связи и массовых коммуникаций
Российской Федерации

Индустриальный партнер



Решаемая проблема

Платформа InnoChain будет обеспечивать принципиально более высокий уровень надежности (за счет формальной верификации) по сравнению с СРР текущего поколения, а также сертифицированную российскую криптографию.

Применение решения (2021 год):

ТРАНСПОРТНАЯ И ЭНЕРГЕТИЧЕСКАЯ ИНФРАСТРУКТУРА

ФИНАНСОВАЯ СФЕРА

ЗДРАВООХРАНЕНИЕ

ОБРАЗОВАНИЕ

ПРОМЫШЛЕННОСТЬ (РОБОТОТЕХНИКА)

ЖИЛИЩНО-КОММУНАЛЬНОЕ ХОЗЯЙСТВО

Основные результаты по окончании проекта

Первая в РФ полностью верифицированная
система распределенного реестра, включающая:

- специализированный язык программирования с верифицированным компилятором
- методы верификации свойств программ
- криптографические методы и протоколы

Не менее **40**
подготовленных специалистов
по программам высшего
образования в области СРР

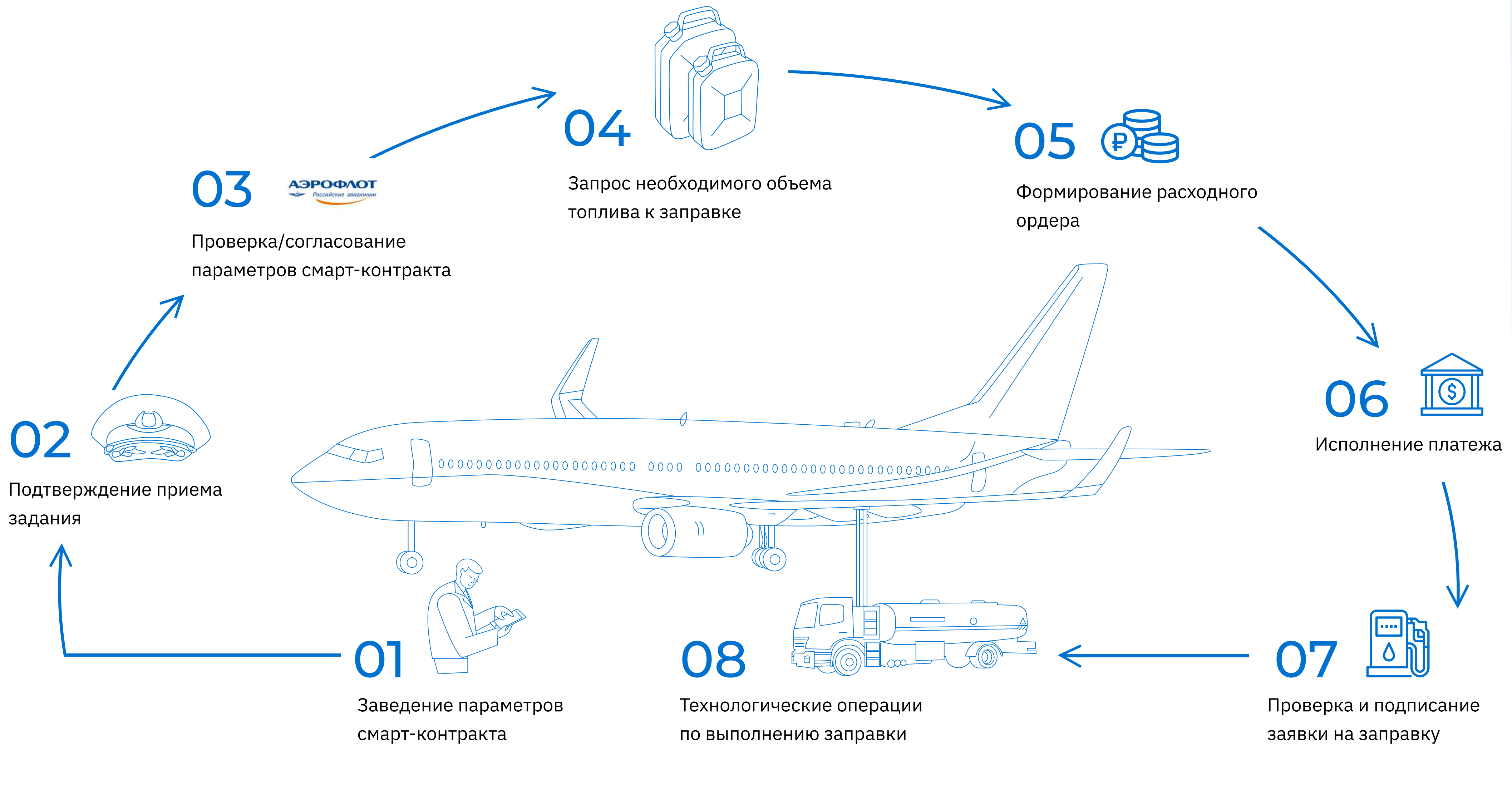
Не менее **9** заявок на выдачу патента

6 полученных патентов

Не менее **10** математических моделей
изделий и процессов

не менее чем в **6** отраслях
реализация проектов

Базовый отраслевой проект



Сокращение времени заправки воздушного судна

До 5 минут После 2 минуты

Сокращение отвлечения денежных средств в случае предоплаты

До 5-30 дней После Мгновенно

Получение авиакомпанией первичных документов по заправке воздушного судна (расходного ордера)

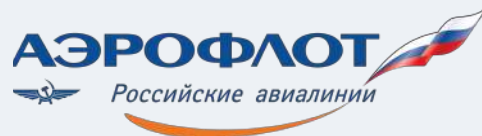
До 1-5 дней После Мгновенно

Дополнительные преимущества

1 Юридически значимый документооборот

2 Полностью автоматическая система расчетов

ТРАНСПОРТНАЯ ИНФРАСТРУКТУРА



- 1. MVP системы заправки воздушных судов, интегрированной с системой распределенного реестра. Интеграция с компаниями-топливозаправщиками (Газпром нефть, Роснефть, Лукойл, Татнефть и др.) и банками (Банк ВТБ, Райффайзен, Сбербанк и др.)
- 2. Программы лояльности (мили, бонусы)
- 3. Закупка услуг и товаров
- 4. Взаимодействие с агентами продаж
- 5. Грузовые перевозки
- 6. Техническое обслуживание и ремонт

ФИНАНСОВЫЕ УСЛУГИ



- 1. Разработка решения для услуг факторинга совместно с крупнейшими холдингами/корпорациями РФ
- 2. Цифровая расчетная система, отвечающая требованиям быстродействия и безопасности
- 3. Разработка и внедрение решений в банковской сфере РФ, согласованных с регулятором, таких как цифровая ипотека, распределенная депозитная система, управление цифровыми финансовыми активами (ЦФА)

ОБРАЗОВАНИЕ



- 1. Учет полного периода обучения/ получения образования с использованием технологии блокчейн
- 2. Разработка единой системы хранения и обработки сквозной информации о полученном образовании для каждого гражданина РФ
- 3. Реализация концепции цифрового диплома международного стандарта на основе отечественного решения распределенного реестра, представляющего собой полноценное портфолио молодого специалиста (полное представление об основных знаниях, достижениях и успехах кандидата на требуемую вакансию), позволяющий усилить уровень защиты документов о высшем образовании и минимизировать количество фальсифицированных документов

СВЯЗЬ



- 1. Разработка платформы для предоставления услуги телемедицины с целью хранения и обработки персональных данных клиентов согласно установленным регламентам в РФ, интеграции с медицинскими и фармакологическими компаниями
- 2. Система хранения, верификации обработки клиентских данных (физ.лица и юр. лица), полученных из большого числа внутренних хранилищ, в том числе и облачных, в интересах Почты России

ГОРОДСКОЕ ХОЗЯЙСТВО



- 1. Контроль сферы ЖКХ
- 2. Голосование и управление общественными местами
- 3. Смарт-контракты как способ экономического взаимодействия автономных устройств внутри городской среды или отдельных домохозяйств

ПРОМЫШЛЕННОСТЬ



- 1. Контроль цепочек поставок с целью увеличения кооперации как внутри одной организации, так и между участниками рынка
- 2. Платформа управлением жизненным циклом выпускаемых изделий
- 3. Создание отдельных элементов «цифрового завода» в рамках концепции «Индустрия 4.0» с целью обмена информацией между конечным заказчиком и производителем для оперативного изменения производственных процессов

ЗДРАВООХРАНЕНИЕ



- 1. Платформа учета и контроля использования рецептурных и наркотических лекарственных средств
- 2. Персональные цифровые медицинские карты с возможностью использования данных как в любом мед.учреждении, так и страховых компаниях (Росгосстрах, СОГАЗ, Ингосстрах, АльфаСтрахование)
- 3. Платформа для учета и контроля в области трансплантологии

Связь программы ЛИЦ с дорожной картой «Системы распределенного реестра»

ЗНАЧИТЕЛЬНОЕ ВЛИЯНИЕ
НА СУБТЕХНОЛОГИЮ «ТЕХНОЛОГИИ
СОЗДАНИЯ И ИСПОЛНЕНИЯ
ДЕЦЕНТРАЛИЗОВАННЫХ ПРИЛОЖЕНИЙ
И СМАРТ-КОНТРАКТОВ»

ВЛИЯНИЕ НА 11 ЦЕЛЕВЫХ ПОКАЗАТЕЛЕЙ
ДОРОЖНОЙ КАРТЫ «СРР»

ЭКСПЕРТЫ ЦЕНТРА СРР УНИВЕРСИТЕТА
ИННОПОЛИС ПРИНИМАЛИ УЧАСТИЕ
В РАЗРАБОТКЕ ДОРОЖНОЙ КАРТЫ

Влияние ЛИЦ на целевые показатели дорожной карты

Показатель	Показатель Дорожной карты развития СЦТ СРР в 2021 году	Целевой показатель Программы ЛИЦ Университета Иннополис в 2021 году
Средний срок интеграции системы в бизнес-процессы, часов	50	10
Средний срок аудита смарт-контрактов, минут	5	3
Количество разработанных децентрализованных приложений и отраслевых решений	100	50
Количество разработчиков смарт-контрактов и децентрализованных приложений	500	100
Количество коммитов в открытых репозиториях исходных кодов	50 000	10 000
Доля цифровизированных бизнес-процессов за счет внедрения смарт-контрактов	30%	30%
Количество инструментов создания смарт-контрактов на естественном языке	15	10
Количество стандартизированных ораклов	100	70
Количество универсальных инструментов создания децентрализованных приложений	15	8
Количество технологических стандартов в части алгоритмизации процессов	100	80
Количество зарегистрированных патентов	80	6

Основная концепция платформы InnoChain

InnoChain — это цифровое решение, обеспечивающее формально-верифицированное функционирование российской системы распределенного реестра

Формальная верификация — это самый мощный современный подход к обеспечению надежности ПО: математическое доказательство свойств надежности с использованием систем компьютерной логики.

5 уровней формальной верификации в ядре InnoChain:

— язык смарт-контрактов

логика смарт-контрактов является гарантированно корректной, исключаются трудозатраты на аудит и ошибки аудита

— компиляция смарт-контрактов

исключаются ошибки виртуальной машины, гарантируется корректность исполнения смарт-контрактов

— алгоритмы узлов CPP с верифицированной компиляцией

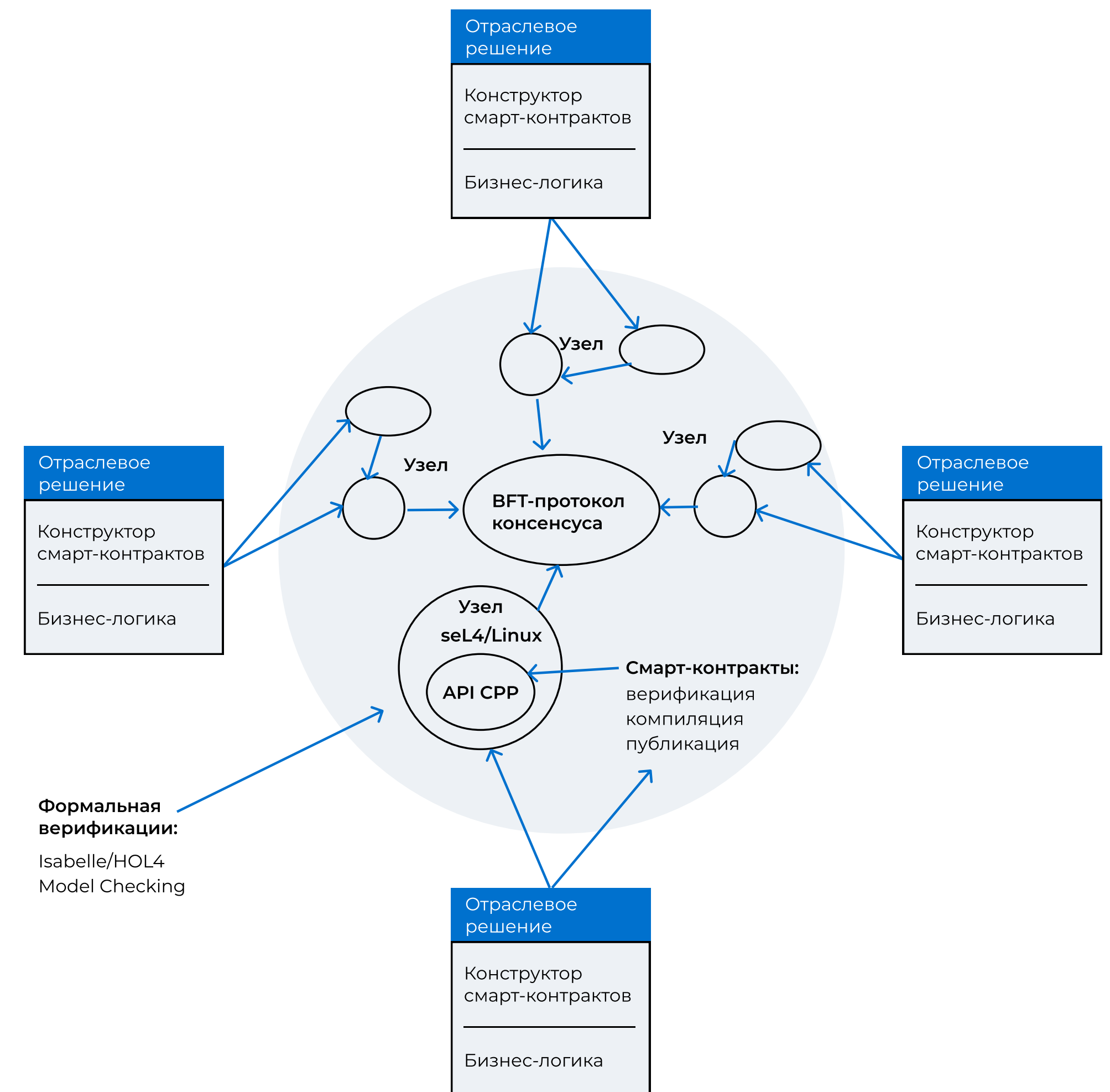
— операционная система (seL4)

исключаются низкоуровневые уязвимости

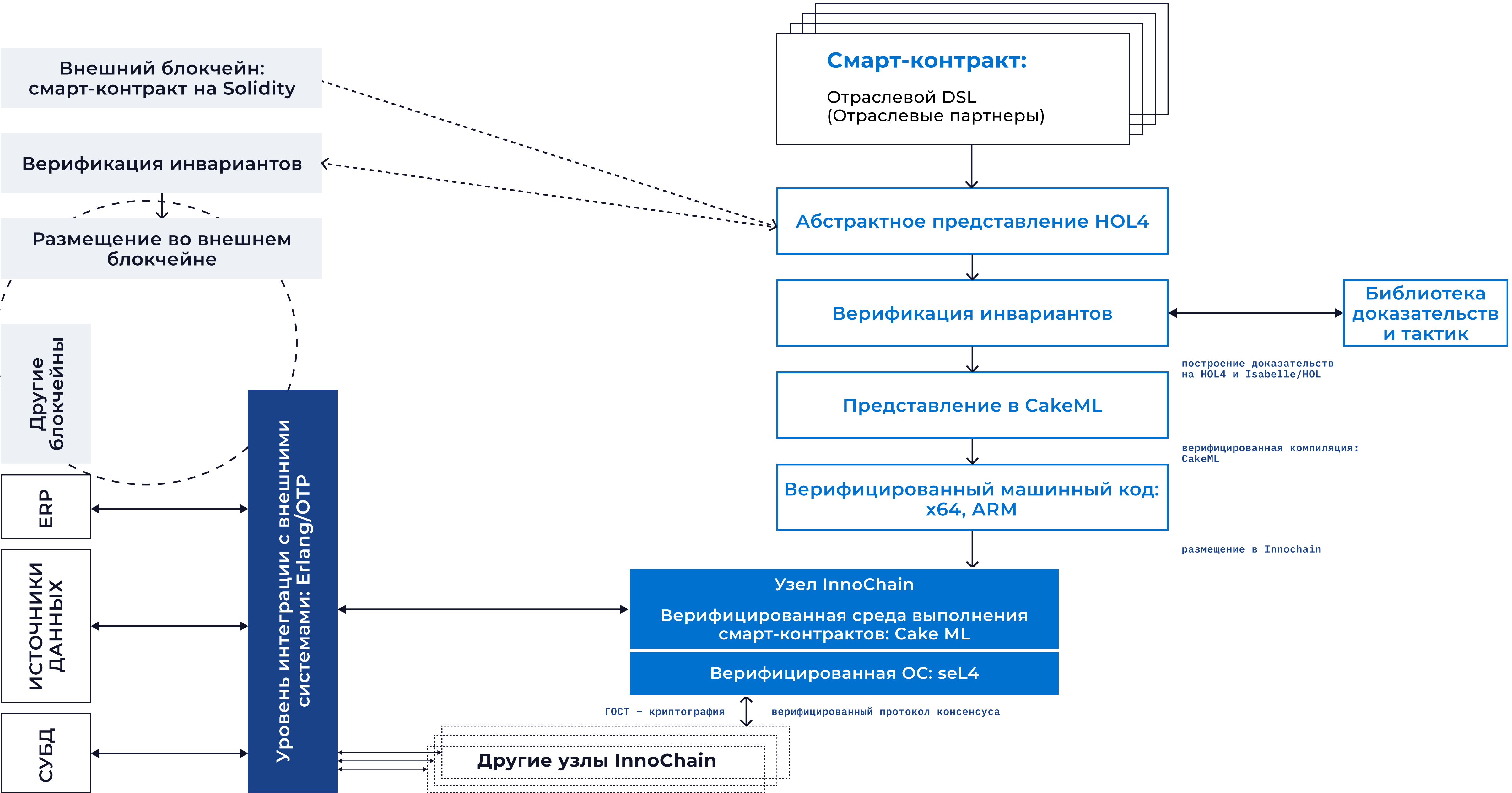
— протокол консенсуса

исключаются атаки на протокол

Высоконадежная интеграция с внешними системами на основе технологий Erlang/OTP



Структура решения InnoChain



Технологии, методы и преимущества InnoChain

Формальная верификация и верифицированное программирование для ядра InnoChain

- Функциональный язык программирования ML с формальной семантикой
- Верифицированный компилятор CakeML для языка ML
- Системы компьютерной логики высших порядков HOL4 и Isabelle/HOL
- Библиотеки доказательств и тактик построения доказательств
- Генераторы кода, используемые для двусторонней интеграции CakeML и HOL4
- Верифицированная операционная система seL4
- Механизмы интеграции CakeML с seL4

Высоконадежные технологии интеграции InnoChain с внешними системами

- Основная технология  Erlang
- Платформа с открытым кодом, 30+ лет успешной эксплуатации в телекоммуникационной индустрии
- Надежность до 99.9999 %
- x10 производительность труда разработчиков
- Поддержка Java, .NET Core и др.

Пальма первенства:

- InnoChain — первая в мире индустриальная СРР с полной формальной верификацией
- Первая полностью российская СРР с открытым кодом и криптографией, сертифицированной в соответствии с ГОСТ
- Одна из первых в мире СРР с нативным исполнением смарт-контрактов (путем компиляции в машинный код)

Спасибо за внимание

ДМИТРИЙ ПЛАХОВ

Руководитель разработки ЛИЦ

d.plakhov@innopolis.ru

+7 (985) 955 00 69

