Доверенная среда смарт-контрактинга и умных пространств вдоль Северного Морского пути

Покровская Н.Н.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина);
Российский государственный педагогический университет им. А.И. Герцена

nnp@ya.ru

Аннотация. **Реализация доверенной среды на примере построения умных пространств Северного Морского пути (СМП) включает создание замкнутого киберфизического контура, в котором инициализация рейса судна в смарт-контракте привязана к цифровым следам, а оплата и самообучения платформенных алгоритмов для уточнения сроков ледокольной проводки практически исключают ошибки, потери времени и утрату данных. В процессе движения телеметрические данные с IoT-датчиков, с криптографической подписью, поступают в реестр, смарт-контракт сверяет показания судна, ледокола и независимых метеоспутников. При выполнении условий происходит исполнение обязательств: оплата ледокольной проводки и корректировка страхового рейтинга. Цифровая среда трансформирует доверие из субъективной социально-правовой категории в объективный, алгоритмически гарантированный параметр цифровой экосистемы. Автоматическое исполнение обязательств отражает независимость от политических настроений, оппортунизма исполнителей, подделки данных, что снижает институциональные барьеры и препятствия для входа стран БРИКС, и прежде всего, Китая, в сотрудничество в рамках коридора СМП.**

Ключевые слова: цифровая экосистема; блокчейн; умное пространство; доверенная среда, инфраструктура

I. Арктика как полигон умного пространства

Северный морской путь (СМП) рассматривается как полигон для применения блокчейна смарт-контрактинга в логистике и социально-экономическом управлении территориями в целом. Экстремальные условия, высокая стоимость ошибки («Север ошибок не прощает», как говорят жители российских северных городов), особая экология Северного Ледовитого океана и условия вечной мерзлоты, участие множества независимых организаций (порты, ледокольный флот, таможня, страховщики, грузоотправители) и вовлечение разных юрисдикций в управление Арктикой в целом (8 стран Арктического Совета) делают неэффективными традиционные формы управления и документооборота.

Включение заинтересованных стран в развитие и эксплуатацию Севера планеты опирается на инжиниринг доверенной среды, при этом роботизация и цифровая трансформация физических процессов (формирование киберфизических систем, CPS) существенно упрощают и облегчают освоение регионов, которые ранее ставили неприемлемые вызовы для их «промышленного» освоения. Если малые народы Севера тысячелетиями вырабатывали способы выживания и жизнеобеспечения в условиях холода, недостаточной инсоляции, ресурсной недостаточности на уровне небольших мобильных групп и гибкого ответа на среду, то устойчивое стабильное функционирование транспортно-логистических узлов и производственных комплексов нуждается в технологиях, обеспечивающих целостный мониторинг пространств огромной площади и своевременное реагирование на основе автоматизированных систем регуляторов.

Интеграционные процессы БРИКС+, евразийского и африканского сотрудничества (начиная с походов купца Афанасия Никитина «за 3 моря» и морских экспедиций Чжэн Хэ для легитимации Юнлэ (Чжу Ди), третьего императора династии Мин, в 1405–1433 гг.), также ставят вопрос о формировании доверенной инфраструктуры.

Заинтересованность Китая и других стран Евразии в освоении арктического побережья континента связана и со стремлением диверсифицировать риски, прежде всего, геоэкономические и военно-политические угрозы при проходе по южным транспортным коридорам. Восточная часть северных территорий континента недостаточно освоена и с точки зрения природных ресурсов: добычи полезных ископаемых; низкой сейсмики для снижения расходов на виброизоляцию оборудования литографии и удешевления выпуска годных кристаллов и продуктов (например, процессоров с высокой плотностью чипов) на Алданском и Анабарском щитах Сибирской платформы; континентального климата с предсказуемой инсоляцией и силой ветра для производства электроэнергии из возобновляемых источников. Достаточно слабая освоенность пространств Арктики одновременно даёт и преимущества институциональной «чистоты», когда нет эффекта «выбранного пути» (path dependency) и затрат на снос и переделку существующих социально-управленческих решений.

Всё это определяет целесообразность реализации умных пространств в Российской Арктике на основе доверенной среды блокчейна и обеспечения цифровой кибер-физической связанности и управляемости.

II. Доверенная среда блокчейна и инфраструктура смарт-контрактинга

Блокчейн-технологии возникли как распределённый («децентрализованный» в понимании отказа от центра) ответ на утрату доверия к централизованным денежно-финансовым властям и посредническим структурам после глобального банковского коллапса (схлопывания кредитно-страхового пузыря) в 2007–2009 гг. Резко вырос спрос на предложенные ещё в 1982–1991 гг. форматы безопасных распределённых реестров (e-cash, Византийская отказоустойчивость, доказательства с нулевым разглашением, Zero-Knowledge Proofs, ZKP,

связанные хэш-цепочки и временные метки, Linked hash chains and timestamping, «клиентская головоломка» и др. математические и вычислительные разработки) [1] в условиях общественной потребности в развитии горизонтальных регулятивных механизмов на основе сетевых платформенных решений.

A. Доверие и инфраструктура доверенной среды

Эффективная институциональная инфраструктура согласования платформенных решений в среде БРИКС опирается на инжиниринг доверия. Доверие как социокультурный механизм снижения транзакционных издержек за счёт усвоения долговременного надёжного и устойчивого действительного опыта соблюдения правил и исполнения взятых обязательств, в вычислительной среде оценивается на основе аудита уязвимостей.

Вместе с тем, с социально-управленческих позиций, доверие выступает результирующим психологическим явлением, которое разворачивается и «выращивается» (deploy & foster) на основе опыта совершения ошибок и интеграции механизмов реагирования на инициативы с учётом «коллективной мудрости», осторожности и культурной инерции, «сопротивления инновациям» в любых форматах, включая заключение международных соглашений и создание интеграционных органов.

Так, например, для признания Китайской Народной Республикой российских стандартов понадобилось несколько десятилетий кропотливого накопления опыта сотрудничества, когда профессионалы из КНР смогли убедиться, что стандартизация в Российской Федерации действительно помогает обеспечивать качество бизнес-процессов и продуктов. Принятие российских норм и документов (ГОСТ Р 57700.37–2021 по компьютерному моделированию и цифровым двойникам и более 300 др. стандартов только в сфере гражданской авиации и двигателестроения), согласование «умных стандартов» отражают многолетнее сотрудничество.

В отличие от традиционных моделей, , полагающихся на субъективную оценку надёжности контрагента и опирающихся на межличностную, организационную и страновую репутацию, инжиниринг доверия переносит гарантии исполнения обязательств в плоскость алгоритмической определённости смарт-контрактов и криптографической неизменности распределенных реестров. Эта парадигма является технологическим ядром архитектуры «умных» пространств, например, трансграничных логистических хабов или цифровых двойников складов, где физический слой связан с когнитивным и доверенным слоями. Социотехнический подход позволяет избегать влияния разночтений, разницы в образовании и компетентности [2] в трактовке базовых институтов, заменяя их единым, верифицируемым машинным кодом, что критически важно для построения суверенных цифровых экосистем.

Таким образом, вопрос доверия расположен на стыке компьютерных наук, экономики и поведенческой психологии, которая занимается проектированием систем, где доверие является не субъективным чувством или социальной нормой, а объективным, проверяемым и алгоритмически гарантированным свойством среды.

В традиционном обществе, как и в префронтальной коре мозга человека доверие, строится на репутации, эмоциях и интуитивной оценке рисков, т.е. опирается на целый набор когнитивных искажений и эвристических ошибок. В цифровых экосистемах это непозволительно медленно и уязвимо. Инжиниринг доверия заменяет это тремя технологическими столпами:

B. Инжиниринг доверия и архитектура умной среды

Детерминированное исполнение умных договоров (автоматизированных программных кодов исполнения перехода прав и ценностей, т.е. смарт-контрактов) связано с тем, что правила взаимодействия, процедуры передачи ценностей и сами права собственности на активы прописаны в коде, на платформах и в цифровых архивах. Доверие смещается с контрагента («по расчёту статистической вероятности, агент заплатит») на техническую и математическую гарантию исполнения («код исполнится автоматически при наступлении условия X»). Этот принцип не работает лишь в тех случаях, когда, например, контейнер погружен на судно, которое попало в шторм или атаковано пиратами, и из порта судно вышло с контейнером, а в другой порт пришло без него или с повреждениями. Именно для таких случаев полезны умное пространство и среда IoT, включая цифровой двойник, например, отслеживающий по всему ходу пути судна по веб-камерам и другим датчикам состояние груза.

В блокчейн-экосистеме ответственность прописана в виде жестких, исполняемых условий (if-then) кода, что снижает риски недопонимания на уровне естественного языка и упрощает преодоление лингвокультурных барьеров, переводя вопросы восприятия поведенческих моделей из категории социокультурных регулятивных норм в категорию конкретных исполняемых действий.

Инжиниринг экосистемы включает код и механизмы управления (Governance). Так, создание консорциумного блокчейна для БРИКС, где узлами управляют доверенные организации из разных стран, а правила обновления протокола (онтологии) принимаются через механизмы голосования, защищенные криптографией.

Архитектура умных пространств представляет собой многоуровневую киберфизическую систему (CPS) [3], которая объединяет физический мир (здания, транспорт, люди, датчики) и цифровой мир (модели, алгоритмы, реестры) в единый управляемый контур. «Умное» пространство (городская агломерация, логистический хаб или промышленная зона) обладает способностью собирать данные, сопоставлять их, обнаруживать отклонения, выявлять закономерности, и автономно или полуавтономно реагировать на изменения.

Ключевые элементы инжиниринга доверенной среды:

- Архитектурный выбор построения входа в сети платформ: консорциум на закрытом (Permissioned, «разрешенном») блокчейне с идентификацией и выдачей прав (например, Hyperledger Fabric или Masterchain) или публичные сети. Для экосистем СМП подходит первый вариант.
- Токеномика и стимулы: Как цифровые активы или репутационные токены мотивируют участников экосистемы действовать честно (связь с теорией игр и равновесием Нэша).
- Интероперабельность (Cross-chain): Инжиниринг мостов между разными блокчейнами (например, между российскими и китайскими платформами),

что напрямую связано с интеграцией СПФС и CIPS.

- Оракулы (Oracles): Механизмы безопасной передачи данных из реального мира (IoT-датчики, системы маркировки типа «Честный ЗНАК») в блокчейн для исполнения смарт-контрактов.
- Когнитивный слой (Cognitive Layer): ИИ и машинное обучение, которые анализируют данные двойников, выявляют аномалии и предлагают управленческие решения (или принимают их автоматически через смарт-контракты).

Умные пространства (логистические коридоры, терминалы, порты) в рамках цифровой экосистемы поставляют данные в блокчейн через доверенные оракулы (trusted oracles), замыкая контур: физическое событие → защищённая передача данных → автоматическое исполнение смарт-контракта.

Выделяют следующие слои архитектуры:

- Физический слой (Physical Layer) включает в себя сенсорное оборудование, собирающее данные (IoT-датчики, камеры и т.п.) и исполнительные механизмы (например, перекрывающие заслонки, терморегуляторы на контейнеровозе, идущем по СМП). Здесь же формируются представления об оборудовании для хранения и обработки данных, выбор между облачными (корпоративными или арендованными) и локальными собственными вычислительными мощностями, между удалённой и присутственной деятельностью сотрудников (например, портовым краном уже десятилетиями управляют не из местного пункта управления, а удалённо из более комфортных по климату мест и с более дешёвой рабочей силой), в частности, с чётким выделением профессиональных функций (наладка, ремонт), которые целесообразно осуществлять удалённо с соблюдением всех требований безопасности и защиты критической информационной инфраструктуры (КИИ).
- Слой бизнес-логики содержит смысл договора, его функцию (Smart Contract Layer), он выполняет формализацию институциональных правил и инфраструктуры соглашений и договорённостей в виде кода. Смарт-контракт исполняет условия (например, оплату ледокольной проводки) только при наступлении объективных событий, которые должны быть обусловлены множеством факторов (страховкой, проверкой таможенных пломб и др.).
- Сетевой слой (Network Layer) включает каналы передачи данных (спутниковая связь, LoRaWAN, в ряде случаев радио, проводная телефонная связь или Bluetooth), обеспечивающие непрерывный поток информации, нередко дублированный.
- Слой данных и криптографического доверия (Trusted Layer) включает распределённые реестры (DLT) и алгоритмы консенсуса.

Выстроенная архитектура позволяет экономить существенные избыточные расходы и снижать риски при реализации транспортно-логистического сервиса СМП.

III. Примеры реализации смарт-контрактинга СМП

В рамках цифровой трансформации государственных и корпоративных систем в Российской Федерации возник целый ряд успешных кейсов, которые зародились и накопили высокий уровень зрелости в ходе «очистки Арктики» госкорпорацией Росатом и развития северных портов и логистических узлов.

A. Автоматизация ледокольной проводки и страхования

Оплата услуг ледокольной проводки и активация страховок требуют длительного документального подтверждения факта оказания услуги в сложных ледовых условиях. Смарт-контракт, привязанный к IoT-датчикам судна и данным гидрометеорологических служб позволяет реализовать модель судна, близкую к понятию цифрового двойника: когда модель фиксирует вход в акваторию СМП и начало проводки конкретным ледоколом, смарт-контракт автоматически инициирует платеж и активирует страховой полис. Это исключает споры и задержки платежей.

B. Сквозной блокчейн-трекинг и «бесшовная» таможня

Груз, идущий из Китая в Европу через Дальний Восток и затем по СМП, пересекает несколько таможенных зон. Бумажные коносаменты и акты могут быть сфальсифицированы. Создание единой платформы распределенного реестра для всех участников цепочки позволяет записывать и хранить в неизменном журнале данные по таким документам, как таможенные декларации, сертификаты происхождения товара, данные по качеству, показатели температуры в рефрижераторах. Это создает неизменяемую историю груза, что позволяет внедрять «зеленый коридор» для таможенного оформления и резко снижает транзакционные издержки.

В случае с Китаем Россия заключила дополнительное соглашение по блокчейн-мониторингу навигационных пломб со связью, позволяющих онлайн отслеживать перемещений опломбированных контейнеров.

C. ESG-логистика и углеродные токены (Зеленая цифровая платформа)

Необходимость подтверждения низкого углеродного следа арктических перевозок для международных рынков связана с возможностью уплаты штрафа при высоких выбросах и, наоборот, с получением льгот при разнообразных выплатах или даже возврата части налоговых платежей при соблюдении экологического законодательства, особенно, в Европейском Союзе.

Использование блокчейна для выпуска и погашения углеродных единиц. Например, компания СИБУР уже неоднократно проводила сделки по приобретению и погашению углеродных токенов в публичном распределенном реестре на Зеленой цифровой платформе (в частности, Сбера) [4], что напрямую применимо к арктическим проектам и логистике СМП.

Для систематизации рассмотренных кейсов можно описать примерный пошаговый алгоритм работы цифрового двойника судна в доверенной среде смарт-контрактов на примере ледокольной проводки и страхования на Северном морском пути (СМП).

В такой экосистеме будут участвовать судовладелец, грузоотправитель, оператор ледокольного флота (например, «Атомфлот» / Росатом), банковские учреждения и страховые компании (андеррайтер арктических рисков). Они могут заключить договор в доверенной платформенной среде в рамках консорциума, закрытой блокчейн-сети, построенной, например, на базе Hyperledger Fabric или Masterchain.

Инициализация и деплой смарт-контракта (Pre-voyage) происходят, когда грузоотправитель ищет транспортный сервис, а судовладелец планирует рейс из Мурманска в китайский порт. В блокчейн-сети разворачивается смарт-контракт, привязанный к цифровому двойнику конкретного судна, в котором прописываются маршрут и контрольные точки (waypoints); тариф на ледокольную проводку (зависит от ледовой обстановки); условия страхового полиса (например, автоматическая выплата при задержке более 48 часов из-за льдов, но *не* из-за поломки судна). Средства грузоотправителя блокируются на условном депонировании (эскроу-счёте) внутри смарт-контракта.

Судно заходит в зону СМП, начинается ледокольная проводка. Датчики судна (GPS / Beidou /ГЛОНАСС, акселерометры, датчики расхода топлива, термодатчики рефрижераторов) собирают телеметрию. Данные не отправляются «как есть». На борту судна (на уровне шлюза, edge-устройства) каждый пакет данных криптографически подписывается закрытым ключом устройства. Это гарантирует, что данные не были подменены при передаче через спутниковую связь. Эти устройства выступают в роли доверенных оракулов (Trusted Oracles).

Перекрестная верификация в распределенном реестре (Consensus) опирается на множественность источников данных: смарт-контракт получает данные не из одного источника, а требует кворума нескольких источников.

Программный код контракта сверяет подписанные данные GPS с судна, подписанные данные телеметрии с ледокола сопровождения, объективные данные метеоспутника о ледовой обстановке в данной точке. Если данные совпадают с условиями, цифровому двойнику присваивается статус «Находится под ледокольной проводкой в зоне X».

Исполнение обязательств (Execution) происходит, когда модель (цифровой двойник) фиксирует событие «Судно вышло из зоны ледовой проводки в чистую воду» (на основе геозоны и данных всех оракулов).

Автоматическое действие смарт-контракта включает оплату, контракт мгновенно и без участия бухгалтеров переводит оговоренную сумму со счета судовладельца на счет оператора ледокольного флота. Код анализирует время в пути. Если оно уложилось в норму с учетом ледовой обстановки, страховой полис автоматически продлевается или фиксируется как «успешно закрытый без рисков». Если произошла вынужденная стоянка из-за льдов, смарт-контракт инициирует микро-выплату за простой. Атомарная транзакция (либо исполняется всё, либо не исполняется ничего) исключает споры, акты сверки, задержки платежей.

Обратная связь и самообучение цифрового двойника опирается на завершённые и верифицированные данные о рейсе (реальный расход топлива, скорость во льдах, точное время проводки), которые анализируются ИИ для обновления и уточнения предиктивной модели двойника.

Для следующего рейса смарт-контракт сможет предложить более точный, персонализированный тариф на страхование и логистику, основанный на реальной, а не заявленной истории судна.

Экосистемный подход позволяет перейти от мозаики фрагментарных цифровых решений к доверенной среде институциональной инфраструктуры [5].

IV. Заключение

Северный морской путь и Российская Арктика в целом предоставляют широкие возможности для апробации инжиниринга доверия умных пространств в масштабах макрорегиона. Экстремальные условия и высокая цена ошибки в арктической логистике делают традиционные бумажные процедуры неэффективными. Внедрение распределенных реестров позволяет создать сквозной блокчейн-трекинг грузов (в частности, в рамках интеграции систем маркировки «Честный знак» и антиконтрафактных систем Alibaba и JD), обеспечивая неизменяемость данных о таможенном оформлении и температурных режимах.

В свою очередь, смарт-контракты, интегрированные с IoT-датчиками судов, автоматизируют расчеты за ледокольную проводку и активацию страховых полисов в режиме реального времени, что прямо закреплено в обновленной Транспортной стратегии РФ. Подобная архитектура «умного» пространства СМП нивелирует кросс-культурные и институциональные барьеры между участниками, заменяя сложные этические понятия криптографически верифицируемым машинным кодом. В контексте БРИКС инжиниринг доверия позволяет странам с разным уровнем институционального развития и разными культурными кодами взаимодействовать в единой цифровой среде.

Список литературы

[1] Sasikumar A., Vairavasundaram S., Kotecha K., Indragandhi V., Logesh R., Selvachandran G., Abraham A. Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things // Future Generation Computer Systems. 2023. Vol. 141. P. 16–27. DOI: 10.1016/j.future.2022.11.002

[2] Слободской А.Л., Теребкова Т.А., Гарин А.К. Цифровое образование и новое технологическое поколение: спрос на новый контент в обучении // Наука о данных: Материалы международной научно-практической конференции, Санкт-Петербург, 5-7 февраля 2020. СПб.: СПбГЭУ, 2020. С. 287-289.

[3] Федоров А.А., Либерман И.В., Корягин С.И., Клачек П.М. Технология проектирования нейро-цифровых экосистем для реализации концепции Индустрия 5.0 // π-Economy. 2021. №3.

[4] Горбашко Е.А., Костин К.Б., Каримова Л.А. Оценка уровня влияния цифровизации Северного морского пути на экономическое развитие арктических регионов // Экономика, предпринимательство и право. 2025. Т. 15, № 5. С. 3557-3578. – DOI 10.18334/epp.15.5.123321.

[5] Гарин А.К., Иванов Д.А., Трапицын С.Ю. Адаптивная цифровая экосистема образовательного учреждения как переход от фрагментарной клиповой мозаики к сети знаний // Инновации и инвестиции. 2026. № 8. С. 320-323.