

Лекция 5. Сквозная цифровая технология «Системы распределенного реестра»

Д.т.н., профессор Гусева А.И.

2025 г.

Системы распределенного реестра

- Технология **систем распределенного реестра** представляет собой новый подход к созданию баз данных, ключевой особенностью которого является отсутствие единого центра управления
- Каждый узел составляет и записывает обновления реестра независимо от других узлов
- В отличие от распределённых баз данных каждый участник системы распределенного реестра хранит всю историю изменений и валидирует добавление любых изменений в систему с помощью алгоритма консенсуса, который математически гарантирует невозможность подделки данных при определённой доле достоверных нод
- Ни один участник не может изменить данные в системе таким образом, что другие участники не узнают об этом

Сквозная цифровая технология «Системы распределенного реестра»

Блокчейн (цепочка блоков) —распределенная база данных, у которой устройства хранения данных не подключены к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок содержит метку времени и ссылку на предыдущий блок

Применение шифрования гарантирует, что пользователи могут изменять только те части цепочки блоков, которыми они «владеют» в том смысле, что у них есть закрытые ключи, без которых запись в файл невозможна. Кроме того, шифрование гарантирует синхронизацию копий распределенной цепочки блоков у всех пользователей

В технологию блокчейн изначально заложена безопасность на уровне базы данных

Концепцию цепочек блоков предложил в 2008 г. Сатоши Накамото (Satoshi Nakamoto). Впервые реализована она была в 2009 г. как компонент цифровой валюты — биткойна, где блокчейн играет роль главного общего реестра для всех операций с биткойнами

Сквозная цифровая технология «Системы распределенного реестра»

Благодаря технологии блокчейна **биткоин стал первой цифровой валютой**, которая решает проблему двойных расходов (в отличие от физических монет или жетонов, электронные файлы могут дублироваться и тратиться дважды) без использования какого-либо авторитетного органа или центрального сервера

Безопасность в технологии блокчейн обеспечивается через децентрализованный сервер, проставляющий метки времени, и одноранговые сетевые соединения. В результате формируется база данных, которая управляется автономно, без единого центра

Это делает цепочки блоков очень удобными для регистрации событий (например, внесения медицинских записей) и операций с данными, управления идентификацией и подтверждения подлинности источника

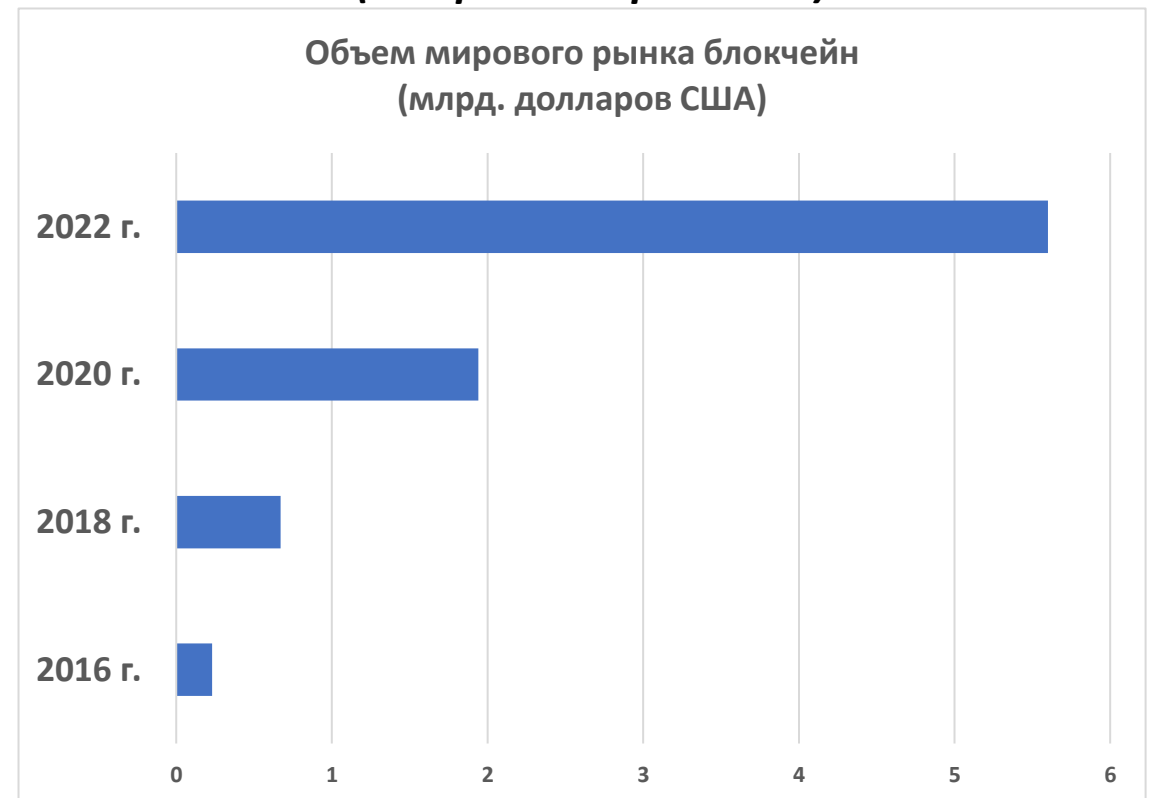
Сквозная цифровая технология «Системы распределенного реестра»

Область применения:

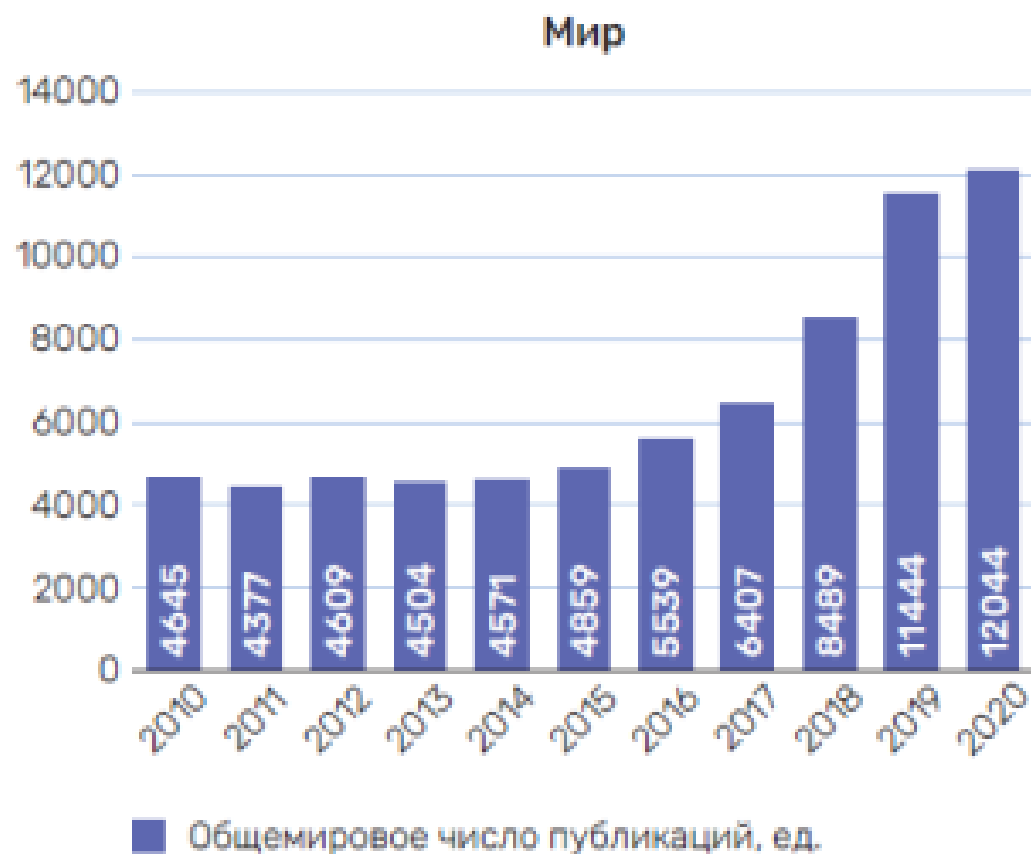
- Финансовая и банковская сфера
- Охрана интеллектуальной собственности
- Денежные переводы на основе криптовалют
- Микроплатежи
- Умные контракты
- Сектор здравоохранения
- Идентификация физических объектов и активов
- Интернет вещей
- Юридические услуги
- Энергетика
- Государственные органы управления, органы обороны и безопасности, международные организации
- Оптимизация внутренних бизнес-процессов отдельных компаний

По оценкам PwC к 2030 году блокчейн-технологии обеспечат рост мировой экономики на \$1,7 трлн.

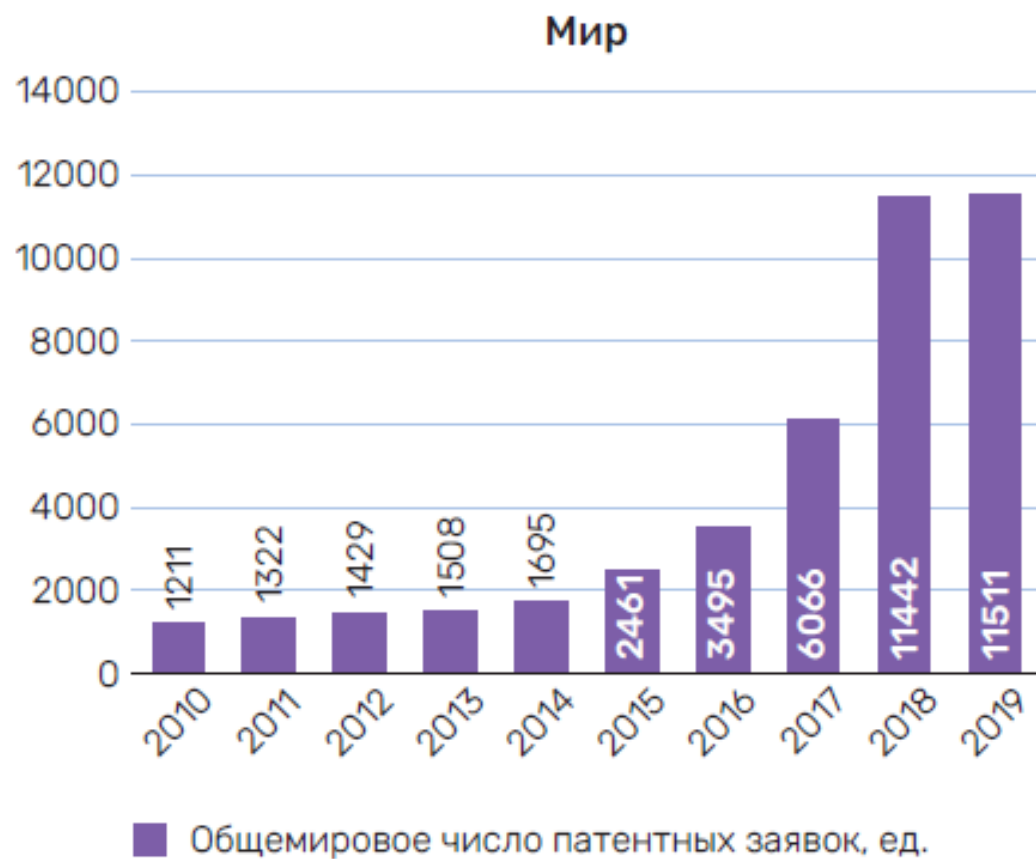
*Объём мирового рынка блокчейн-технологий
(млрд. долларов США)*



Ключевые показатели публикационной активности



Ключевые показатели патентной активности

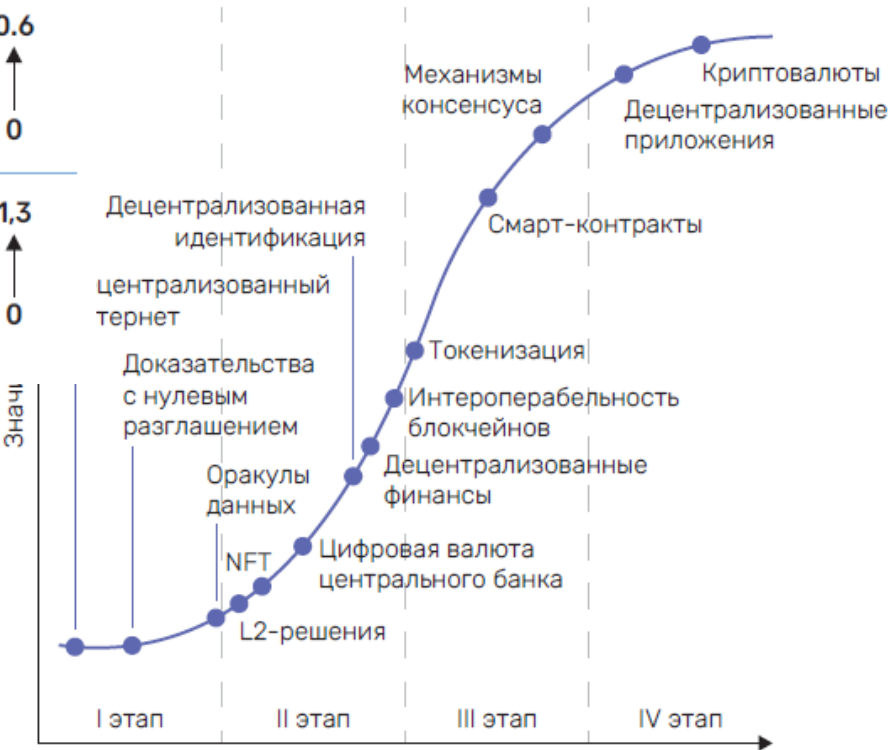


Основные показатели публикационной и патентной активности по группам технологий

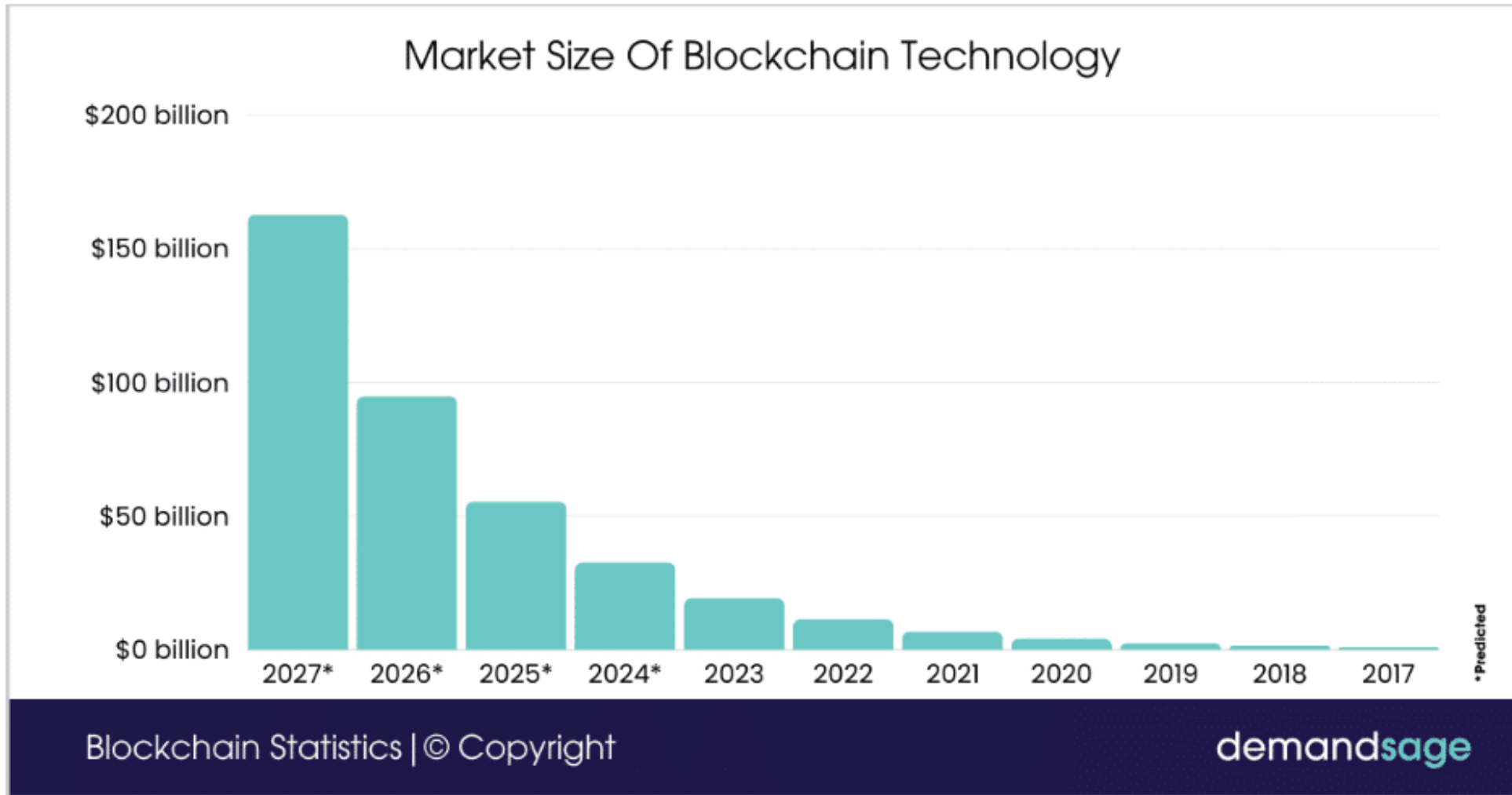
Научные публикации					Патентные заявки				
		Мир	Россия	Доля России, %		Мир	Россия	Доля России, %	
Технологии уровня протокола, структуры данных и алгоритмов достижения консенсуса	2020	4041	113	2,8	2019	10641	18	0,2	
	2015	1413	17	↑	2015	1735	9	↑	
	2010	1135	7	0,6	2010	604	2	0,3	
Технологии уровня сетевого взаимодействия	2020	4949	96	1,9	2019	1075	6	0,6	
	2015	2685	32	↑	2015	465	3	↑	
	2010	3287	17	0,5	2010	471	0	0	
Технологии уровня приложений, услуг и дополнительных компонентов	2020	3765	64	1,7	2019	158	2	1,3	
	2015	526	7	↑	2015	56	0	↑	
	2010	15	0	0	2010	1	0	0	

Кривая технологической зрелости

- **Уровень протокола, структуры данных и алгоритмов достижения консенсуса** (включая децентрализованный интернет, L2-решения, доказательства с нулевым разглашением, интероперабельность блокчейнов, механизм консенсуса)
- **Уровень сетевого взаимодействия** (включая децентрализованную идентификацию)
- **Уровень приложений, услуг и дополнительных компонентов** (включая токенизацию, оракулы данных, децентрализованные финансы, криптовалюты, цифровую валюту центрального банка, NFT, децентрализованные приложения, смарт-контракты)

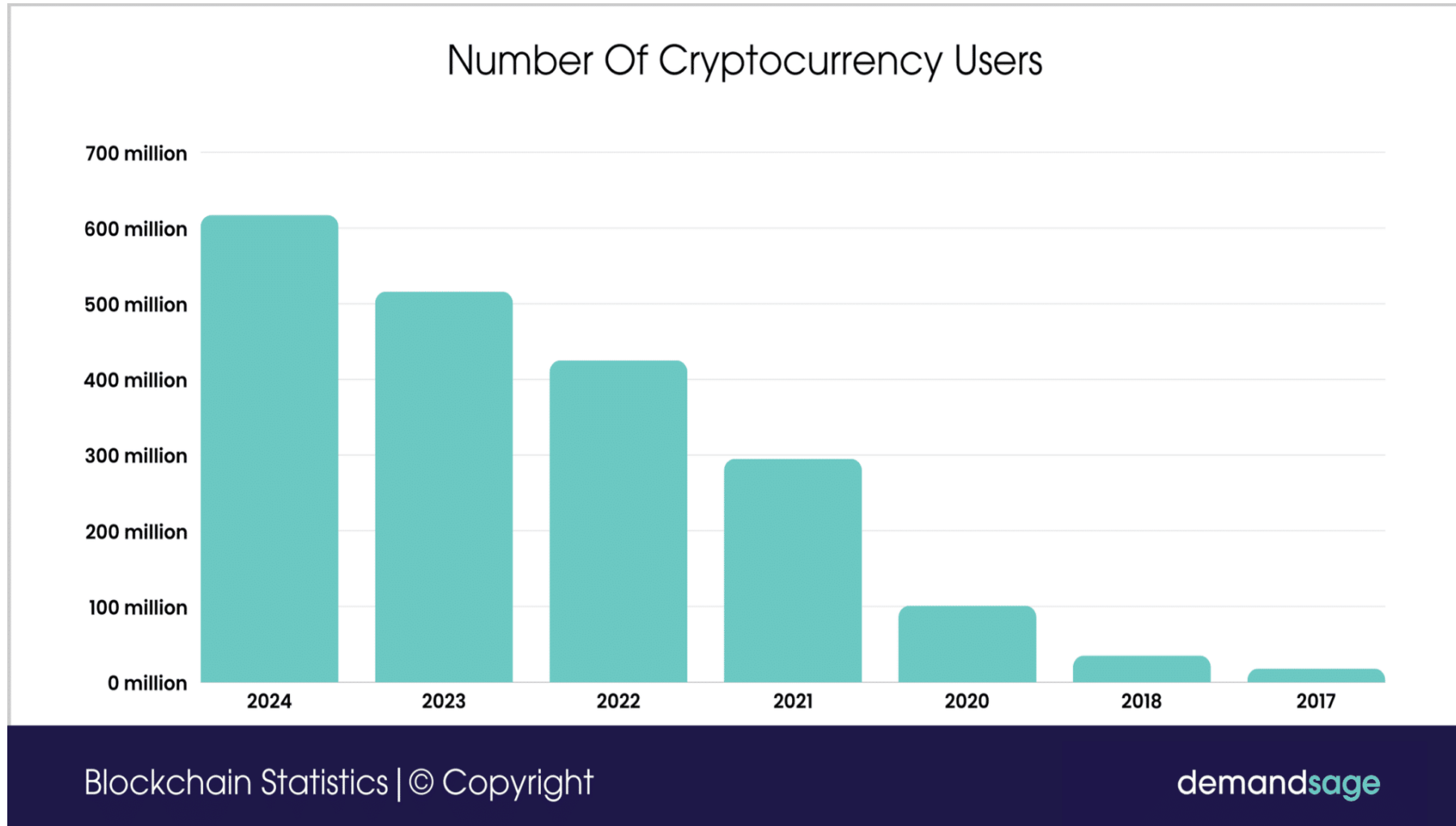


Мировой рынок блокчейна



- По данным на август 2024 года, мировой рынок блокчейн-технологий оценивается в \$26,91 млрд долларов
- Ожидается, что к 2034 году он достигнет \$1 879,3 млрд долларов

Мировой рынок блокчейна



- По состоянию на 2024 год в мире насчитывается более 617 миллионов пользователей криптовалют
- Это прирост в 100 миллионов пользователей криптовалют по сравнению с 2023 годом

Семь главных трендов на рынке блокчейна (2023-2024 гг.)

- **1. Внедрение блокчейна в корпоративном сегменте**
- **2. Развитие децентрализованных финансовых сервисов (DeFi)**
- **3. Невзаимозаменяемые токены (NFT)**
- **4. Масштабируемость и совместимость в области блокчейна**
- **5. Интеграция с традиционными системами**
- **6. Развитие концепции «блокчейн как услуга» (BaaS)**
- **7. Государственные инициативы в области блокчейна**

Системы распределенного реестра: субтехнологии (ДК)

- **Технологии обеспечения целостности и непротиворечивости данных (консенсус)** – совокупность методов и инструментов, направленных на приведение в соответствие имеющихся данных в децентрализованной сети к единой внутренней логике и структуре по заранее определённым правилам, а также обеспечение синхронизации и согласования данных между узлами децентрализованной сети
- **Технологии создания и исполнения децентрализованных приложений и смарт-контрактов** – совокупность методов и инструментов, направленных на создание приложений, обеспечивающих взаимодействие неограниченного количества участников распределённой системы, и на разработку, поддержание и выполнение компьютерных алгоритмов, предназначенных для автоматизации процессов исполнения контрактов. Децентрализованные приложения обладают прозрачной и открытой логикой, обеспечивающей гарантированное исполнение заданных функций в рамках систем распределенного реестра
- **Технологии организации и синхронизации данных** – совокупность методов и инструментов, направленных на определение, организацию и усовершенствование взаимосвязей между частями и элементами распределённых баз данных, а также на обеспечение их согласованности и приведение к соответствию

Связь с другими сквозными цифровыми технологиями

Сквозные цифровые технологии	Характер взаимосвязи ССР с остальными СЦТ
Нейротехнологии и искусственный интеллект	Совместно с субтехнологиями «Обработка естественного языка», «Распознавание и синтез речи» и «Рекомендательные системы и системы поддержки принятия решений» в качестве среды обмена обезличенными данными для обучения алгоритмов данных субтехнологий и безопасного обмена самими алгоритмами
Компоненты робототехники и сенсорики	Платформенные решения на базе систем распределенного реестра могут выступать инфраструктурой обмена данными между устройствами субтехнологии «Сенсорное оборудование»

Связь с другими сквозными цифровыми технологиями

Сквозные цифровые технологии	Характер взаимосвязи ССР с остальными СЦТ
Большие данные	Могут использоваться с целью хранения и обмена данными для субтехнологий «Обработка и утилизация данных» и «Обогащение данных»
Новые производственные технологии	Могут использоваться для управления транзакциями и обработки данных

Развитие сквозной цифровой технологии: задачи

1. Развитие технологий организации и синхронизации данных - определяет уровень организации взаимосвязей между частями и элементами распределенных баз данных, а также обеспечивает их согласованность и приведение к соответствию

- Сократить среднее время, необходимое для подтверждения блоков
- Снизить требования вычислительным мощностям полных нод
- Уменьшить время развертывания полной ноды
- Увеличить количество стандартизированных протоколов для обращения к внешним данным и интероперабельности

Развитие сквозной цифровой технологии: задачи

2. Развитие технологий обеспечения консенсуса - определяет целостность и непротиворечивость данных, а также устойчивость к атакам и надежность систем распределённого реестра

- Снизить уровень чувствительности пропускной способности систем распределенного реестра к количеству и географической распределенности полных нод
- Повысить уровень децентрализации распределения вычислительных мощностей и ресурсов систем распределенного реестра
- Увеличить пропускную способность
- Повысить кибербезопасность систем в части обеспечения защиты от захвата ресурсов/вычислительных мощностей сети

Развитие сквозной цифровой технологии: задачи

3. Развитие создания и исполнения децентрализованных приложений и смарт-контрактов - определяет возможности подключения неограниченного количества участников распределенной сети, а также цифровизации процессов исполнения контрактов

- Сократить сроки интеграции систем в бизнес-процессы
- Сократить средний срок аудита смарт-контрактов
- Увеличить количество поддерживаемых системами распределенного реестра языков программирования

Развитие сквозной цифровой технологии: задачи

4. Разработка инструментов, расширяющих функционал систем распределенного реестра - определяет возможности применения технологии в бизнес-процессах, отсутствие данных инструментов существенно сужает потенциал использования технологии

- Создать инструменты для разработки смарт-контрактов на естественном языке
- Создать и стандартизировать ораклы (инструменты обращения систем распределенного реестра к внешним данным для исполнения условий смарт-контрактов)
- Создать инструменты автоматизированного аудита смарт-контрактов
- Создать инструменты разработки смарт-контрактов и децентрализованных приложений
- Создать инструменты интероперабельности
- Создать инструменты развертывания нод на маломощных системах, например, смартфонах и IoT-устройствах

Развитие сквозной цифровой технологии: задачи

5. Внедрение решений в отрасли - определяет уровень развития и потенциал масштабирования отечественных отраслевых платформ распределенного реестра в приоритетных отраслях

- Деятельность финансовая и страховая
- Транспортировка и хранение
- Государственное управление
- Деятельность в области здравоохранения
- Обработывающие производства

Технологии организации и синхронизации данных: технологические задачи

- 1. Сократить среднее время, необходимое для подтверждения блоков
- 2. Снизить требования вычислительным мощностям полных нод
- 3. Увеличить количество стандартизированных протоколов для обращения к внешним данным и интероперабельности

Показатель (технологический, рыночный)	2019	2021	2024
Среднее время, необходимое для подтверждения блока, мин.	8,2	< 1	<0.02
Средний срок развертывания полной ноды, ч.	96	30	1
Доля полностью интероперабельных платформ, соответствующих ГОСТ в части криптографии	5%	25%	80%
Количество запатентованных технологий организации и синхронизации данных	0	15	50
Доля компаний, обладающих полными нодами в системах распределенного реестра	<1%	10%	55%
Количество системных архитекторов с опытом в области построения распределенных систем	100	500	3 000

Технологии обеспечения целостности и непротиворечивости данных (консенсус): технологические задачи

Снизить уровень чувствительности пропускной способности систем распределенного реестра к количеству и географической распределенности полных нод

Повысить уровень децентрализации распределения вычислительных мощностей и ресурсов систем распределенного реестра

Увеличить пропускную способность

Повысить кибербезопасность систем в части обеспечения защиты от захвата ресурсов/вычислительных мощностей сети

Показатель (технологический, рыночный)	2019	2021	2024
Количество транзакций в секунду	1 000	5 000	100 000
Защита от захвата вычислительных мощностей, ресурсов, % захваченных мощностей от общего числа	51%	51%	76%
Количество полных нод	5	2 500	10 000
Количество запатентованных консенсус алгоритмов	0	15	50
Доля платформ распределенного реестра, сертифицированных по ГОСТ	0%	10%	55%
Количество выпускаемых специалистов в области криптографических алгоритмов, используемых в системах распределенного реестра, в год	250	750	2 500

Технологии создания и исполнения децентрализованных приложений и смарт-контрактов : технологические задачи

Сократить сроки интеграции систем в бизнес-процессы

Сократить средний срок аудита смарт-контрактов

Увеличить количество поддерживаемых системами распределенного реестра языков программирования

Показатель (технологический, рыночный)	2019	2021	2024
Средний срок интеграции системы в бизнес-процессы, ч.	120	50	< 10
Средний срок аудита смарт-контрактов на предмет отсутствия критических уязвимостей, мин	120	5	< 1
Количество разработанных децентрализованных приложений и отраслевых решений на базе платформ распределенного реестра	15	100	500
Количество разработчиков смарт-контрактов и децентрализованных приложений	100	500	3 000
Количество коммитов в открытых репозиториях исходных кодов систем распределенного реестра	18 900	50 000	100 000
Доля цифровизированных бизнес-процессов за счет внедрения смарт-контрактов	5%	30%	75%
Количество сервис-провайдеров систем распределенного реестра в приоритетных отраслях	15	150	500

Риски технологии Системы распределенного реестра



Ожидаемые эффекты от развития технологии

Эффект	Достижения
Технологическое лидерство	Обеспечить независимость финансовой инфраструктуры Российской Федерации от зарубежных решений, повысить надежность и кибербезопасность финансовой инфраструктуры. Прогнозируемое сокращение количества сбоев финансовой инфраструктуры - 50% к 2024 году
	Обеспечить рост безопасности процессов хранения и обмена персональными медицинскими данными. Прогнозируемое сокращение количества случаев утечки персональных медицинских данных - 50% к 2024 году;
	Повысить доступность и надежность государственных информационных систем (ГИС), увеличить их защищенность от кибератак. Прогнозируемое сокращение времени технического обслуживания в год - 30% к 2024 году.

Ожидаемые эффекты от развития технологии

Эффект	Достижения
Экономическое развитие	Достичь прямого экономического эффекта, выраженного как сумму дополнительной выручки и сокращению издержек за счет цифровизации процессов, минимизации количества посредников. Прогнозируемый совокупный объем - 782 млрд руб. к 2024 году
	Достичь косвенного экономического эффекта, выраженного в форме сокращения объема теневой экономики и оборота контрафактной продукции за счет обеспечения прозрачности, неизменности и автоматизированной актуализации данных на уровне. Прогнозируемый совокупный объем - 853 млрд руб. к 2024 году

Ожидаемые эффекты от развития технологии

Эффект	Достижения
Социальный прогресс	Повысить доступность финансовых услуг для наименее обеспеченных слоев населения и сократить комиссии на электронные банковские операции для конечных пользователей. Прогнозируемый эффект - 100% населения используют банковские услуги к 2024 году
	Получать государственные услуги в реальном времени и обеспечить неизменность и прозрачность данных при предоставлении различных государственных услуг. Прогнозируемый рост доверия населения к государственным услугам - 30% к 2024 году
	Сократить оборот контрафактных лекарств и улучшить здоровье населения за счет сокращения незаконного оборота рецептурных лекарств и рецептов. Прогнозируемое сокращение случаев заболеваний в результате приема контрафактных лекарств - 30% к 2024 году

Возможности использования блокчейна в BFSI

BFSI (банковское дело, финансовые услуги и страхование) — отрасль включает предприятия, предлагающие различные финансовые продукты и услуги

В отрасль **BFSI** входят:

- универсальные банки, предоставляющие разнообразные финансовые услуги
 - предприятия, работающие в одной или нескольких из этих финансовых отраслей
 - страховые фирмы
 - коммерческие банки
 - небанковские финансовые компании
 - кооперативы
 - пенсионные фонды
 - паевые инвестиционные фонды
- и другие более мелкие финансовые учреждения

Возможности использования блокчейна в BFSI

1. БЛОКЧЕЙН ДЛЯ ТРАНСГРАНИЧНЫХ МЕЖБАНКОВСКИХ РАСЧЕТОВ

Применение блокчейна в финансовой сфере позволяет резко увеличить скорость трансграничных расчетов и снизить их стоимость за счет устранения посредников - коммерческих банков, клиринговых палат и т.д.

Практика крупных банков, присоединившихся к внедрению блокчейна для трансграничных расчетов, показывает, что блокчейн позволяет сократить время обработки транзакций с нескольких дней до нескольких секунд и снизить комиссию за обработку с 5-30% до 2-3%

Отметим, что в данном случае криптовалюта выступает не в качестве основной платежной валюты, а в качестве фиатно-крипто-фиатного моста, обеспечивающего трансграничную обработку транзакций в сети блокчейн

Возможности использования блокчейна в BFSI

2. БЛОКЧЕЙН ДЛЯ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Блокчейн обеспечивает автоматизацию выполнения финансовых операций и ведения учета на основе смарт-контрактов, что позволяет финансовым компаниям повысить производительность труда сотрудников и добиться значительной экономии операционных затрат. Чем сложнее и более документоемкий процесс, тем более впечатляющие результаты дает автоматизация на основе блокчейна

Например, при внедрении в процесс урегулирования страховых случаев смарт-контракты позволили сократить затраты в 5 раз и увеличить скорость обработки претензий примерно в 3 раза

Фактически, условия практически любого юридически обязывающего финансового соглашения могут быть формализованы в смарт-контрактах в качестве правил, обеспечивающих автоматическое выполнение тех или иных бизнес-действий

Появление прокси-контрактов позволило эффективно решить проблему обновляемости смарт-контрактов. С помощью прокси-контрактов можно легко корректировать логику смарт-контракта в соответствии с изменяющимися условиями соглашения

Возможности использования блокчейна в BFSI

БЛОКЧЕЙН ДЛЯ ФИНАНСОВОГО ДОКУМЕНТООБОРОТА

Финансовый документооборот - еще одна важная область, в которой блокчейн способен принести пользу финансовым организациям

Технология может обеспечить сквозное отслеживание любых действий пользователей, связанных с созданием, редактированием, просмотром, копированием и передачей третьим лицам финансовых документов

Это позволяет обеспечить безопасное и прозрачное хранение и обмен финансовыми документами, что способствует повышению доверия между финансовыми организациями и их клиентами.

Возможности использования блокчейна в BFSI

3. БЛОКЧЕЙН ДЛЯ ВЫЯВЛЕНИЯ МОШЕННИЧЕСТВА

Наибольшая доля рисков мошенничества, с которыми сталкивается сектор BFSI, исходит от сотрудников. В 2022-2023 годах почти 52% случаев мошенничества, о которых сообщают финансовые учреждения РФ, связаны с внутренним персоналом

Блокчейн помогает своевременно обнаруживать и предотвращать недобросовестное поведение пользователей, предоставляя неизменяемые записи со временными метками обо всех бизнес-транзакциях и манипуляциях с финансовыми данными и документами

Логика автоматизированного выявления мошенничества может быть закодирована в смарт-контрактах, что позволяет исключить участие человека и обеспечить неподкупную проверку на мошенничество. Если блокчейн работает в паре с искусственным интеллектом, выявление мошенничества может осуществляться полностью автоматически и с высокой точностью

Возможности использования блокчейна в BFSI

4. БЛОКЧЕЙН ДЛЯ ЦИФРОВОЙ ПРОВЕРКИ ЛИЧНОСТИ

Объем краж личных данных с 2017 года вырос в 5 раз и в 2024 году приведет к потерям в 56 млрд руб. Это подталкивает финансовые организации к поиску действенного метода борьбы с мошенничеством, позволяющего избежать финансовых и репутационных рисков. Здесь блокчейн также является сильным помощником

С помощью технологии блокчейн уникальная информация о клиенте может быть представлена в виде децентрализованного идентификатора или НМТ, зашифрована и записана в устойчивую к взлому распределенную бухгалтерскую книгу

Хранилище токенизированных цифровых идентификаторов на основе блокчейна обеспечивает единый источник истины для проверки личности клиента, гарантируя при этом полную безопасность конфиденциальных персональных данных.

Возможности использования блокчейна в BFSI

5. БЛОКЧЕЙН ДЛЯ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ КҮС/AML

Еще одним примером использования блокчейна для поставщиков финансовых услуг является обеспечение соответствия требованиям КҮС/AML

Автоматизация проверок на соответствие требованиям с помощью смарт-контрактов устраняет трудоемкую и подверженную ошибкам ручную проверку личности клиента в соответствии с требованиями КҮС/AML

Устойчивость блокчейна к взлому обеспечивает достоверность данных, предоставляемых клиентами организации, что позволяет предотвратить несанкционированный доступ к финансовым услугам.

Возможности использования блокчейна в BFSI

6. БЛОКЧЕЙН ДЛЯ ПРИНЯТИЯ КОРПОРАТИВНЫХ РЕШЕНИЙ

Учитывая сложную иерархию управления в крупных финансовых организациях, принятие решений по стратегическим бизнес-операциям не всегда бывает простым

Блокчейн позволяет оптимизировать процесс принятия совместных решений и укрепить доверие между всеми заинтересованными сторонами организации

В основе технологии блокчейн лежит высоконадежная и неподкупная модель электронного голосования

Благодаря токенизированным правам управления и алгоритмической проверке и подсчету голосов поставщики финансовых услуг получают достоверное голосование и повышают производительность и вовлеченность менеджеров

Возможности использования блокчейна в BFSI

7. БЛОКЧЕЙН ДЛЯ ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ УСЛУГ

В условиях глобального перехода к более широкому охвату населения финансовыми услугами традиционные игроки рынка BFSI должны охватить недостаточно обслуживаемое население и сделать свои услуги доступными для людей с самыми низкими доходами

Именно здесь DeFi (децентрализованные финансы) преуспевает, а традиционные финансы отстают

Своей популярностью DeFi обязана высокой доступности блокчейна. Эта технология позволяет обеспечить легкий круглосуточный доступ к основным финансовым услугам без ограничений по местонахождению и кредитной истории

Традиционные банки и поставщики финансовых услуг, очевидно, не готовы полностью перейти на эту технологию. Однако мы видим, как растет число финансовых институтов, принимающих решения на базе blockchain или сотрудничающих с платформами DeFi для расширения охвата клиентов и повышения доступности своих услуг

Помимо социальной составляющей, BFSI-компании руководствуются и прагматическими соображениями: выход на быстро развивающийся рынок DeFi и охват большей клиентской базы открывают новые возможности для получения прибыли и помогают диверсифицировать риски

Примеры использования технологии

- **Национальный расчетный депозитарий** (входит в группу «Московская биржа») внедряет блокчейн в финансовую инфраструктуру для проведения сделок с ценными бумагами, ведения документации и др.
- **ПАО «Сбербанк»** выполняет проект по переводу всех банковских расчетов на блокчейн. Лаборатория блокчейна разрабатывает проекты для ипотечного кредитования, факторинга, страхования и аккредитивов. Со второго полугодия 2020 г. ПАО «Сбербанк» начал промышленную эксплуатацию системы учета электронных закладных по сделкам с недвижимостью с использованием систем банка и российской национальной блокчейн-платформы Мастерчейн
- **ПАО «ГМК "Норильский никель"»** внедрило решение на базе TRP для упрощения торговли сырьем. Компания выпускает токены, обеспеченные палладием, кобальтом и медью, и продает их производителям. Кроме того, на блокчейне ведется учет полезных ископаемых

Примеры использования технологии

- **ОАО «РЖД» и Maersk** заключили соглашение о взаимодействии в области развития цифровых сервисов для перевозок с использованием TPR и их продвижения на рынок мультимодальных перевозок. Блокчейн также внедряется в сервисном обслуживании локомотивов: используются смарт-контракты, обеспечивающие автоматическое исполнение условий договора
- **S7 Airlines** через блокчейн-платформу продает авиабилеты и взаимодействует с ведущими банками
- **ПАО «Владимирский химический завод» (ВХЗ)** создает блокчейн-платформу для фиксации выбросов парниковых газов
- **ПАО «Газпром нефть»** организует на блокчейне логистические процессы, включая отслеживание перемещения грузов, и продажу топлива. Кроме того, компания разработала собственную блокчейн-систему Smart Fuel для авиазаправок