



 **НИПС**
НОВОСИБИРСКИЙ ИНСТИТУТ
ПРОГРАММНЫХ СИСТЕМ


Development



Blockchain

Consortium of Mining Companies



Об объединении



ПАО «НИПС» с 2018 года входит в контур управления компании АО «Концерн «Автоматика» Государственной корпорации «Ростех».
В штате 116 специалистов, из них 60 разработчиков.

Основные компетенции

- Разработка общесистемного и специального ПО, в том числе для отечественных аппаратных платформ
- Разработка автоматизированных систем управления
- Разработка прикладных информационных систем
- Блокчейн-разработка.

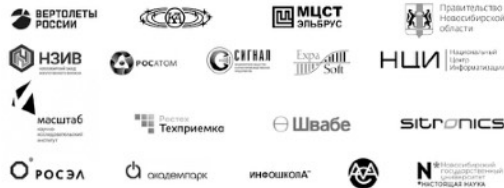
Интеллектуальная собственность НИПС

- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну №0082474
- Лицензия на разработку криптографических средств №0015589
- Сертификат ISO-9001-2008
- Сертификат соответствия СДС.234-2018
- Свидетельство регистрации платформы веб-сайтов «Кираса» №2017610238
- Свидетельство регистрации программной платформы «Premis 4.0» №2016613073 и отдельных модулей платформы «Premis 4.0»

Программное обеспечение
«Информационная система управления недвижимым имуществом «Premis» включено в Единый реестр российских программ для ЭВМ и баз данных (приказ Минкомсвязи РФ № 426).



Наши партнеры



Acryl development – крупнейшая в мире компания, предоставляющая полный цикл услуг в сфере блокчейн-технологий. Мы разрабатываем и внедряем передовые программные и аппаратные решения, позволяющие предприятиям, частным лицам, а также государственным и другим организациям перемещать цифровые активы через блокчейн без риска потери информации. Наши экспертные знания и опыт обеспечивают нашим клиентам успешную, доступную, быструю, безопасную и экономически выгодную связь с блокчейном. Компания Acryl занимается развитием технологии блокчейн на глобальном уровне. В партнерстве с НИПС - наше объединение лидирует в интеграции блокчейн-технологий во все сферы современного цифрового мира.

Предпосылки внедрения технологии блокчейн в нефте-газовой отрасли

Особенность нефтегазовых компаний - большой объем физических активов, высокая стоимость принятия инвестиционных решений, высокие риски принятия операционных решений, значительные размеры инвестиционных проектов и критическая важность управления цепочкой снабжения. В рамках модернизации бизнес-процессов происходит тотальная цифровизация и превращение каждой компании и каждого бизнес-процесса в "процессы, основанные на данных" (data-driven), создавая информационные потоки, в том числе потоки данных о регистрации состояния/происхождения физических объектов, что и является местом применения блокчейн-протоколов.



Предпосылки внедрения технологии блокчейн в нефте-газовой отрасли



Blockchain - распределенная база данных, защищенная криптографическими методами. Ресурсодобывающие организации создают единый «источник правды», позволяющий отследить все события с участием различных элементов производственных процессов, что дает возможность избежать кропотливой ручной работы, сверяя данные. Такой подход избавляет от ненужной траты времени на сверки и упрощает поиск данных в случае, если они запрашиваются регулирующими или контролирующими органами. Полный аудиторский след формируется в режиме реального времени в процессе обработки транзакций как побочный продукт использования технологии Blockchain. Аудитор получает доступ ко всей необходимой информации в режиме реального времени. Преимущества перед существующими трудоемкими процессами очевидны.

Точки применения технологии Blockchain в нефте-газовой отрасли

- **Управление запасами и активами** — регистрация состояния/происхождения материалов/запасов/сырья;
- **Транспорт, логистика, управление цепочками поставок** — регистрация состояния при сборе информации с датчиков и сенсоров;
- **Трейдинг и сбыт** — регистрация изменений и удостоверение прав собственности, торговое финансирование;
- **Без клиринговая торговля;**
- **Оптимизация закупок и сбыта** — оптимизация идентификации поставщиков, подписания закупочных договоров, аудит и отслеживание транзакций;
- **Удостоверение и отслеживание происхождения товаров;**
- **Оптимизация документооборота;**
- **Токенизация физических активов и ценных бумаг;**
- **Оптимизация внутренних экономических и бизнес процессов**



Real mining DLT infrastructure Consortium of Mining Companies



Real mining DLT infrastructure — это реализация архитектурного подхода к созданию экосистемы Consortium of Mining Companies

Подобная реализация позволяет компаниям консорциума выбрать оптимальное сочетание технологий, с учетом собственной специфики.

Кроме того, такая структура позволяет менять компоненты, не затрагивая никаких зависимостей.

Публичный Blockchain	Приватный Blockchain	Гибридная реализация
При реализации на публичных Blockchain-платформах, таких как Bitcoin, Ethereum и других, компании консорциума самостоятельно определяют стек протоколов взаимодействия и интеграции в экосистему Consortium of Mining Companies.	Компании консорциума использующие приватный (корпоративный) блокчейн определяют политику взаимодействия с внешним контуром согласно собственной бизнес логики.	Возможность кастомизации узлов корпоративного консорциума используя доступные преимущества публичных распределенных реестров.

Компоненты DLT infrastructure

Базовые технологические решения

Экосистема **Consortium of Mining Companies** построена на технологии использования криплетов.

Криплеты — основные строительные блоки, позволяющие создать промежуточный слой в архитектуре с защитой Blockchain. Учитывая распределенный характер Blockchain, этот промежуточный слой обычно функционирует как облачный сервис.

В Blockchain версий 1.0 и 2.0 для взаимодействия с внешними данными или событиями (время, показатели рынка, вес и др.) применяются **оракулы**. При этом не существует стандартного способа для безопасного встраивания данных из оракула, что может быть проблемой для SmartContract с несколькими участниками. Вызов кода или данных вне SmartContract или Blockchain снижает уровень доверия, угрожая подлинности зависимых транзакций. Решить эту проблему призваны криплеты.



Компоненты DLT infrastructure

Базовые технологические решения

Криплеты — это код за пределами цепочки, который пишется на любом языке и выполняется в безопасном контейнере. Обращаться к нему можно с помощью защищенных каналов. Криплеты можно использовать в SmartContract и системах UTXO, когда необходимо получить дополнительный функционал или информацию. Такую возможность предоставляют «делегаты шифрования» (CryptoDelegate) или адаптеры.

CryptoDelegate — это функция в виртуальной машине SmartContract, которая вызывает криплет из кода SmartContract, создавая безопасный контейнер для транзакций. Криплеты регистрируются на уровне узла $host^1$. Разработчики затем ссылаются на них или создают их автоматически.

Если для SmartContract требуется криплет, вызывается CryptoDelegate. В код можно включить атрибуты, показывающие, что ответственность за выполнение алгоритма в этой точке передается CryptoDelegate. Например, если одно из свойств SmartContract должно быть зашифровано и отображаться только для сторон этого контракта, можно применить атрибут, подобный следующему:



***[encryptField="ContractSignersOnly"]
uint public trade_amount = 0;***

Атрибут указывает, что поле должно быть зашифровано, но не указывает, как именно.

Компоненты DLT infrastructure

Базовые технологические решения

2 основных типа криплетов: Utility и Contract.



Криплеты Utility — основная часть структуры Blockchain. Они обеспечивают операции, такие как шифрование, события по дате и времени, доступ к внешним данным и идентификация. У каждого криплета Utility есть идентификатор и подтвержденная подпись, которые регистрируются для использования в облаке. Операторы способны обнаруживать криплеты и использовать их в SmartContract для большей надежности транзакций.

Криплеты Contract — полноценный механизм делегирования, который выступает в качестве суппората SmartContract за пределами цепочки. Эти криплеты содержат всю логику выполнения и надежно хранят данные типа SmartContract. Криплеты Contract привязаны к своим SmartContract и генерируются при включении нового контракта в Blockchain. Поскольку криплеты Contract не выполняются в виртуальной машине, они не запускаются на всех узлах Blockchain. Они могут работать параллельно и в вертикально масштабируемых системах, если это необходимо для повышения производительности.

Криплеты Contract могут запускаться как автономные агенты вне цепочки. Криплеты Contract будут полезны для консорциумов, в рамках которых SmartContract подписываются известными контрагентами.

Компоненты DLT infrastructure Real mining Blockchain PLATFORM

Real mining Blockchain PLATFORM — это «платформа распределенного реестра для Consortium of Mining Companies», которая представляет собой традиционное промежуточное ПО с тем исключением, что Real mining Blockchain PLATFORM может работать на глобальном уровне через свои интерфейсы API или в рамках модели «Blockchain как сервис» (BaaS).

ОСНОВНЫЕ СЛУЖБЫ

-Identity and Certificate Services (Службы удостоверений и сертификатов).

Эти службы обеспечивают регистрацию криплетов и применение политик, а также позволяют проверять подлинность организаций, ключевых сделок, контрактов. Поэтому они могут стать платформой для других служб, что позволяет создавать вертикально интегрированные сервисы, такие как службы KYC (know your customer – «знай своего клиента»), средства регистрации, объединения активов и т. д.

-Encryption Services (Службы шифрования).

Эти службы обеспечивают частичное шифрование полезной нагрузки или шифрование на «уровне поля» для транзакций в Blockchain с использованием различных схем шифрования (гомоморфное шифрование, пороговая криптосистема и т. д.). Такой подход позволяет держать в тайне те сведения, которые должны быть доступны только инвесторам и контрагентам, а также регулирующим органам.

-Cryptlet Services (Службы криплетов).

Это проверенный хостинг для криплетов, вызываемых через делегатов в SmartContract или UTXO-адаптерах. Такие сервисы, как службы определения местоположения, подтверждения доверительных отношений, а также безопасные изолированные контейнеры, предоставляют среду выполнения для криплетов, написанных на любом языке, что обеспечивает их выполнение. Спецификации делегатов, адаптеров и криплетов открыты и доступны для сообщества, то есть их можно будет реализовать в других распределенных реестрах.



Компоненты DLT infrastructure Real mining Blockchain PLATFORM

Real mining Blockchain PLATFORM

Поскольку ценность сети распределенного реестра возрастает с увеличением количества разных участников, становится очевидным, что Blockchain-консорциумы будут доминировать в этой сфере. В связи с этим возникает необходимость обеспечения взаимодействия. Real mining Blockchain PLATFORM избавляет Consortium of Mining Companies от необходимости прорабатывать требования к управлению и операциям, конфиденциальности, проверке подлинности, управлению ключами и совершенствованию модели выполнения.

ОСНОВНЫЕ СЛУЖБЫ

-Blockchain Gateway Services (Службы Blockchain-шлюзов).

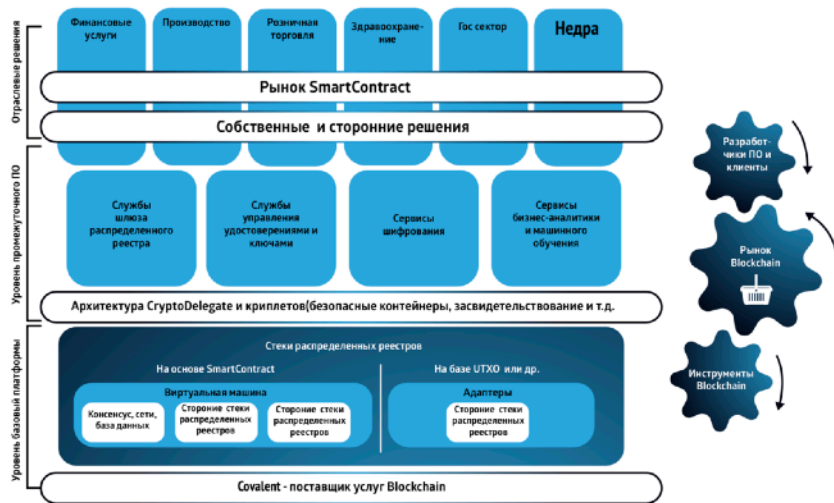
Это службы-посредники, позволяющие передавать контракты SmartContract и токенизированные объекты между разными системами распределенных реестров. Эти службы обеспечивают целостность транзакций между разными реестрами, например при передаче финансовых инструментов в цепочке поставок, охватывающей несколько Blockchain.

-Data Services (Службы данных).

Это ключевые службы для работы с данными, такие как распределенные файловые системы (IPFS, Storj, Acryl и т. д.) для данных за пределами цепочки. На эти данные ссылаются с использованием открытых ключей. Это службы аудита, расширенной аналитики, машинного обучения и создания информационных панелей для SmartContract, Blockchain, инвесторов, «Consortium Maining Company» и регулирующих органов.

-Management and Operations (Управление и операции).

Это инструменты для развертывания, управления и работы с распределенными реестрами «Consortium of Mining Companies». Их использование привносит во все процессы корпоративную организованность, которой так не хватает на современном рынке ресурсодобычи.



Сравнение публичных Blockchain

Название	Ethereum	NEO	LSK	EOS	Acryl	Graphene
Токен	ETH	NEO	LSK	EOS	ACRYL	BTS
Дата запуска	24/07/14	01/06/14	04/05/16	02/07/17	13/01/19	12/01/16
Поддержка языков	Solidity	C#, Java, NET, Kotlin, Python	Javascript	Javascript	Scala	C++
Консенсус	PoW/PoS	PoS	DPoS	DPoS	LPoS	DPoS
TPS, p/s	15	1000	5	100000	8000	100000
Время формирования блока, с	15	15	10	0.5	60	1.5
Dapps	Да	Да	Да	Да	Да	Нет
SDK	Да	Да	Да	Да	Да	Да
Atomic swaps	Нет	Нет	Нет	Нет	В процессе	Нет
Sidechain	Да	Да	Да	Нет	Нет	Нет
Smart contracts	Да	Да	Нет	Да	Да	Да
Размер команды	159	61	36	49	30	11

Сравнение характеристик приватных Blockchain

Название	Ethereum	Hyperledger Fabric	Corda	Acryl (RMBP DLT)
Штаб-квартира	Цуг, Швейцария	Worldwide	США, Нью-Йорк	Россия, Новосибирск
Область применения	C2C, B2C	B2B	Финансовые транзакции	C2C, B2B, B2C, B2G, G2G, C2G, G2C
Консенсус	PoW	PBFT, Нотариальные ноды	Нотариальные ноды	LPoS, PoA
Особенности консенсуса	Требуется майнинг Casper Implementation PoS	Подключаемый консенсус	В консенсусе участвуют только стороны, указанные в транзакции	PoS - на основе формируемых в системе токенов PoA - заданные администратором ноды
Возможность создания централизованной публичной распределенной сети	нет	да	да	да

Сравнение характеристик приватных Blockchain

Название	Ethereum	Hyperledger Fabric	Corda	Acryl (RMBP DLT)
Возможность создания централизованной приватной (с ограниченным числом участников) распределенной сети	нет	да	да	да
Ролевая модель для внесения транзакций	нет	есть	нет	есть
Конфиденциальность (возможность ограничения доступа к части информации)	нет	да	да	да
Возможность использования криптографии по ГОСТ и УКЭП	нет	есть, но требуются доработки	нет	есть
Смартконтракты, язык программирования	smart contract - Solidity	API - Go, Java, JavaScript	smart contract - Java + Kotlin	RUST, Scala (API), docker smart contract



Сравнение характеристик приватных Blockchain

Название	Ethereum	Hyperledger Fabric	Corda	Acryl (RMBP DLT)
Возможность работы без внутренней валюты	нет	да	нет	да
Возможность выпуска токенов	да	да	нет	да
Оценка пропускной способности (tps)	текущий - 15 tps	N/A	N/A	минимум 5000 tps
Возможность использования криптографии по ГОСТ и УКЭП	нет	есть, но требуются доработки	нет	есть
Смартконтракты, язык программирования	smart contract - Solidity	API - Go, Java, JavaScript	smart contract - Java + Kotlin	RUST, Scala (API), docker smart contract

Дальнейшие шаги

1. **Аналитика бизнес-процессов** — Совместное выявление главных кандидатов на реинжиниринг с целью переноса всей или частичной информации на блокчейн
2. **Проработка блокчейн - решения** — Подготовка архитектурных и технологических предложений по реализации в рамках существующего ИТ ландшафта
3. **Разработка блокчейн - решения** — Программирование в соответствии с сформированным решением
4. **Внедрение и мониторинг** — Внедрение результатов деятельности в существующие бизнес-процессы в ограниченном масштабе. Контроль и мониторинг функционирования

Наши контакты

Брызгалов Виктор
Руководитель Центра блокчейн разработок

тел.: +79529303040
e-mail: Nips@nips.ru
telegram: @VictorDeveloper

