



УНИКАЛЬНАЯ ПЛАТФОРМА ДЛЯ СОЗДАНИЯ ПРИВАТНЫХ БЛОКЧЕЙНОВ

Наш продукт



Для обеспечения безопасности используется криптография по стандарту ГОСТ
Продукт находится в стадии получения заключения о корректности встраивания СКЗИ

Решаем задачи

1000

транзакций
в секунду



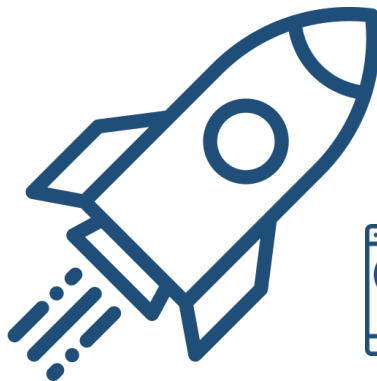
Высокая скорость
обработки
транзакций



Большая гибкость
администрирования системы
за счет разграничения прав



Управление доступностью информации.
Приватная информация доступна валидаторам,
выполняющим роль регуляторов в системе,
а также всем участникам данной транзакции
Для всех остальных данная информация
остаётся недоступной

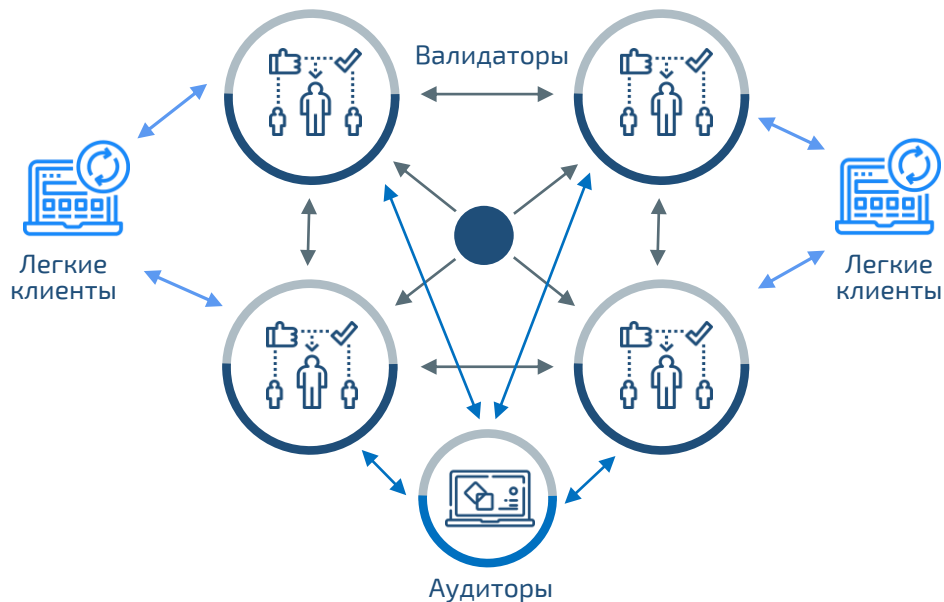


Умная обработка транзакций
с программируемой логикой
и возможностью модификации
под конкретную задачу



Защищенная передача
данных благодаря
использованию СКЗИ

Архитектура платформы



Валидаторы

- Держит полную копию блокчейна
- Обеспечивает надежность сети
- Участвует в формировании консенсуса
- Принимает и осуществляет записи в блокчейн



Аудитор

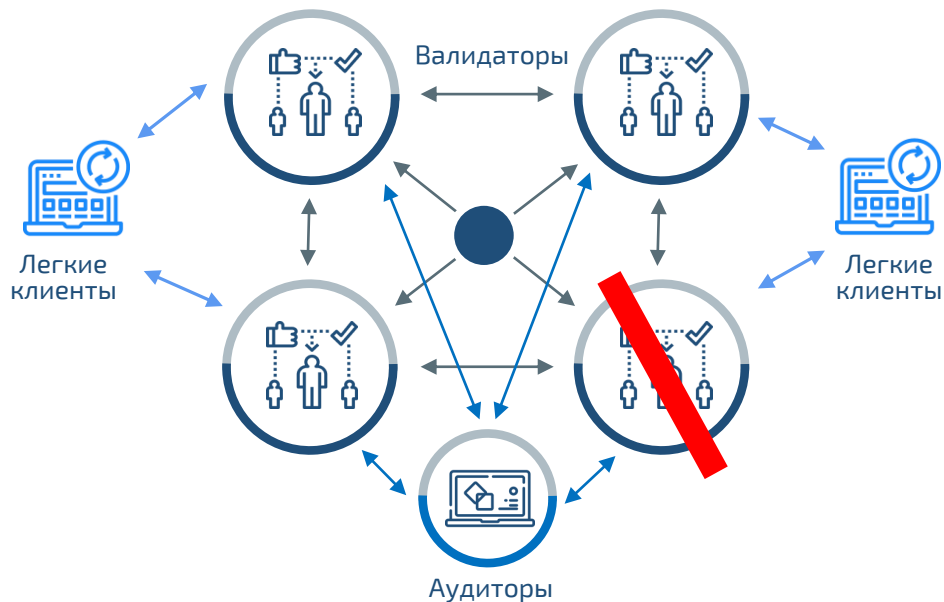
- Держит полную копию блокчейна
- Не участвует в формировании консенсуса
- Полностью проверяет корректность данных



Легкие клиенты

- Взаимодействие с узлами блокчейна
- Представляет собой приложения или веб-сервер

Архитектура платформы



Валидаторы

Держит полную копию блокчейна
Обеспечивает надежность сети
Участвует в формировании консенсуса
Принимает и осуществляет записи в блокчейн



Аудитор

Держит полную копию блокчейна
Не участвует в формировании консенсуса
Полностью проверяет корректность данных



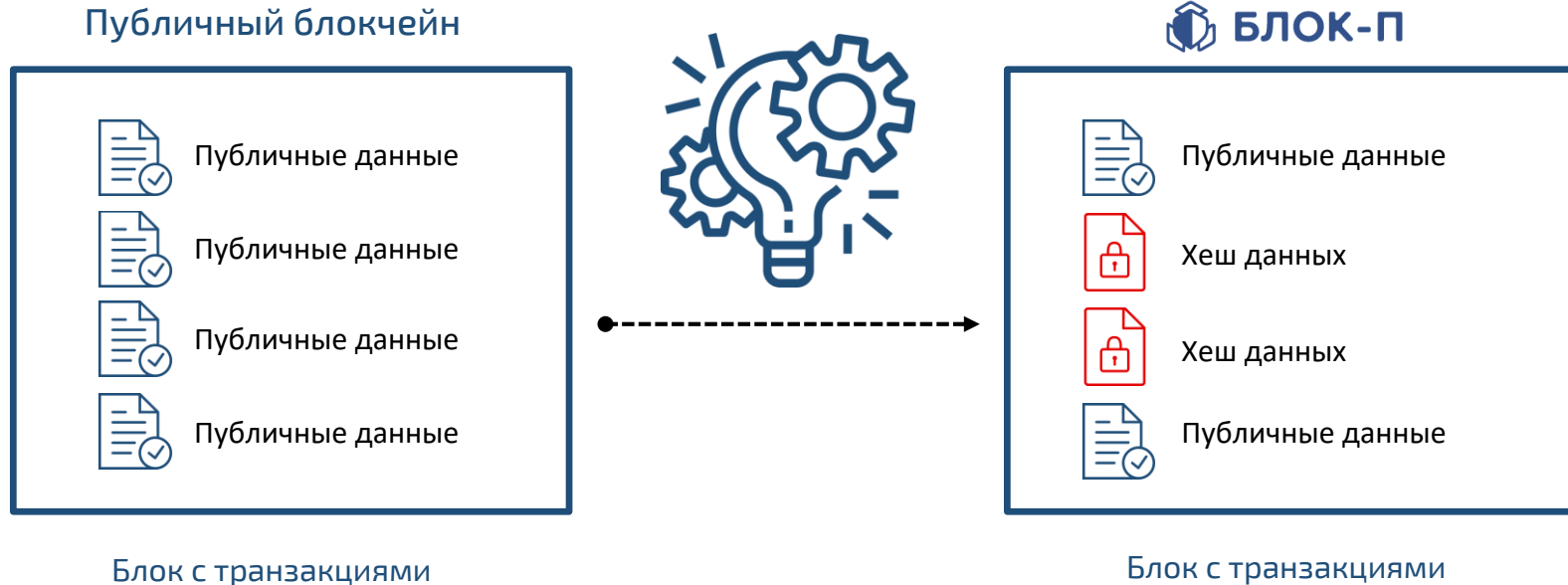
Легкие клиенты

Взаимодействие с узлами блокчейна
Представляет собой приложения или веб-сервер

Приватные транзакции

Вводится новый тип транзакций - приватные транзакции

Для данного типа транзакций тело будет доставляться отдельно, таким образом, тело транзакции смогут получить только непосредственные участники транзакции и валидаторы



Алгоритм распространения транзакции

Формирование транзакции



Алгоритм распространения транзакции

Отправка хэша и тела транзакции валидаторам



Алгоритм распространения транзакции

Получение транзакции валидаторами



Алгоритм распространения транзакции

Проверка всех условий, как у публичной транзакции



Алгоритм распространения транзакции

Хэш транзакции попадает в блок и рассылается на все узлы



Алгоритм распространения транзакции

Тело транзакции рассылается на необходимые узлы



Алгоритм распространения транзакции

Аудиторы обрабатывают блоки




Алгоритм распространения транзакции

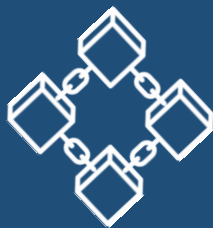
Необходимые узлы получили тело транзакции и обновляют свою базу данных



Криптография



В качестве
приватных ключей
выступают ключи
из сертификатов



Подпись данных
происходит через
СКЗИ КриптоПро

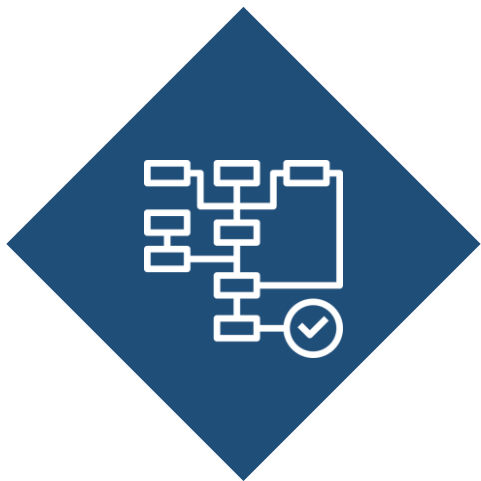
ВСЕ
соединения
защищены с помощью
протокола TLS
реализованным
в СКЗИ
Криптопро



Стандарты криптографии в нашем продукте:

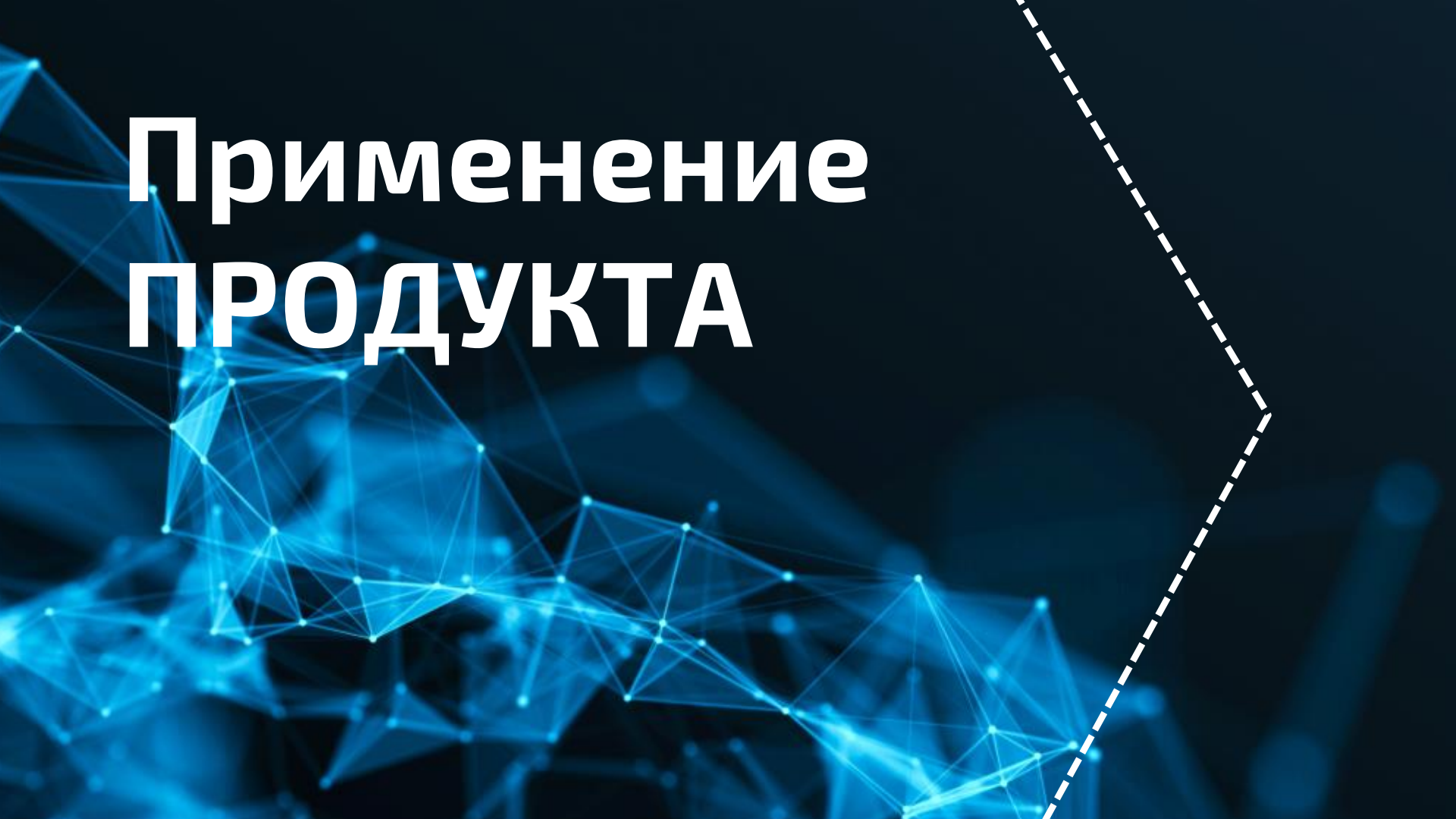
ГОСТ Р 34.10-2012 - для асимметричного шифрования и подписи данных





Очистка блокчейна

- 1** Валидатор отправляет транзакцию на очистку блокчейна
Логика данной транзакции прописывается отдельно
(можно удалить как все данные, так и часть)
- 2** Далее, каждый узел удаляет данные в блокчейне
и все существующие транзакции
- 3** Блоки начинают создаваться с нулевого блока, при
этом сохраняя предыдущие данные
- 4** При подключении новых узлов, состояние данных
блокчейна до очистки отправляется узлу

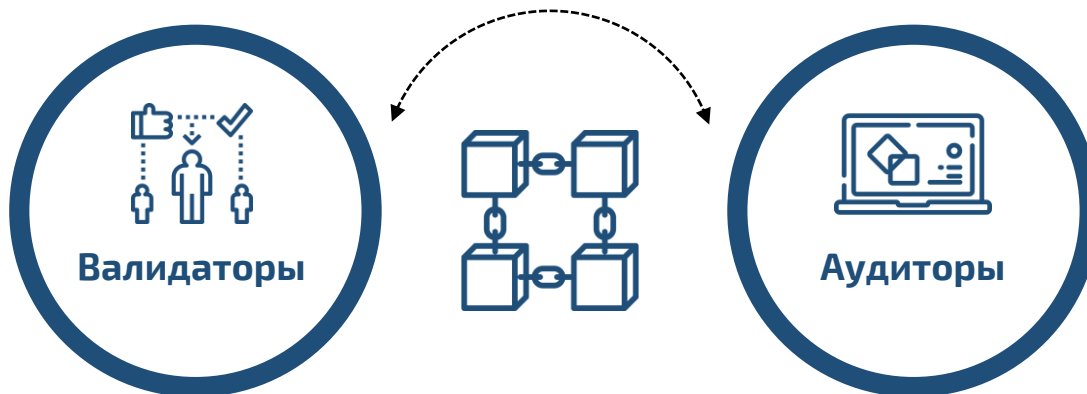
The background features a complex network of glowing blue nodes and connecting lines, creating a sense of digital connectivity. A prominent white dashed arrow points from the top right towards the center of the image, framing the text.

Применение ПРОДУКТА

Создание блокчейна



Применение



Валидаторы

Аудиторы

Узлы валидаторы - заинтересованы в корректности работы платформы
Им доступны все данные и они валидируют все транзакции
На роль валидаторов подходят:
регуляторы
крупные игроки

Узлы аудиторы - базовые участники платформы, доступны только те данные, которые к ним относятся
На роль аудиторов подходят узлы, которым не должны быть доступны все данные на платформе, при этом заинтересованные в актуальности и надежности своих данных