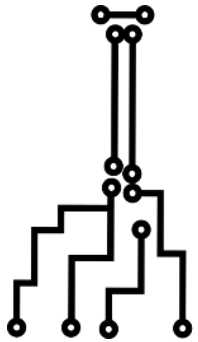
Платформа Б

Распределенная блокчейн-платформа для хранения и обмена данными



SolarLab>_

О компании-разработчике

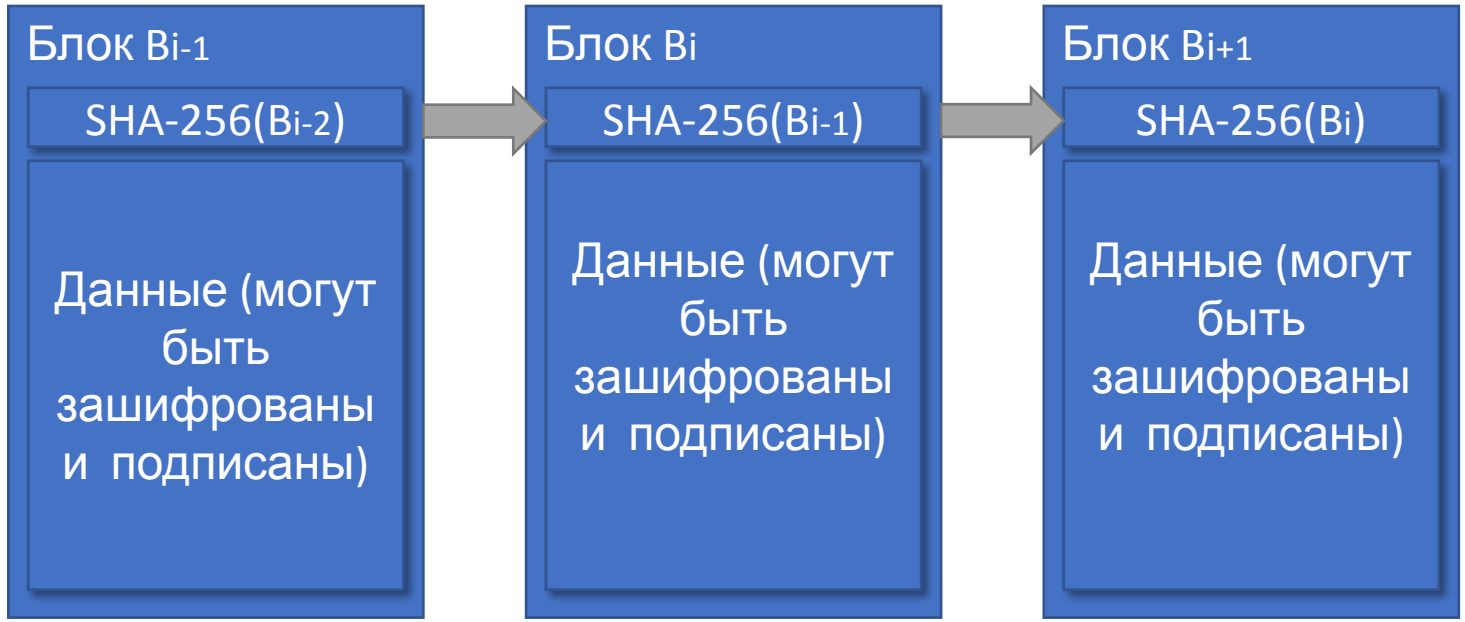
ООО СоларЛаб

- Финансовые технологии и госзакупки:
  - РТС-Тендер – торговые площадки по 44ФЗ, 223ФЗ, 615ППРФ, ЗМО, Имущественным торгам;
  - Мобильные приложения для РТС-Тендер (iOS, Android);
  - b2bpoint.ru – поиск по закупкам;
- Электронный документооборот:
  - Финтендер-Крипто – федеральный оператор ЭДО;
- Перспективные технологии (уже в продуктиве):
  - Блокчейн - платформа для хранения и обмена данными;
  - Боты – для поиска закупок и технической поддержки (партнерство с Microsoft);
  - Технологии машинного обучения – профилирование пользователей и генерация рекомендаций по участию в торгах;

Что такое блокчейн?

- Блокчейн – безопасный распределенный реестр с общим доступом:
  - Децентрализация;
  - Распределенная (p2p) технология;
  - Криптографическое подтверждение;
  - Неизменяемость данных;
  - Бездоверительность (отсутствие необходимости в доверенном центре).
- Применение
  - Частный (наиболее известный) случай – реестры платежных транзакций;
  - Общий случай - любые реестры неизменяемой информации.
  - Еще более общий подход – разделяемая информационная среда, основа Глобальной Виртуальной Машины.

Цепочка блоков



- Каждый новый блок информации содержит хэш от предыдущего
- Это обеспечивает контроль изменений и неизменяемость данных

Технологические основы блокчейна

- Хранение данных в цепочке блоков
  - Неизменность
- Обмен новыми данными для включения в цепочку по распределенному p2p протоколу (подобно технологии BitTorrent)
  - Распределенность
- Включение данных в цепочку только после их валидации на непротиворечивость
  - Криптографическое подтверждение авторитетности источника данных
  - Валидация и запись в цепочку проводится параллельно на всех узлах, при этом правила системы стимулируют честное поведение валидаторов с помощью вознаграждения за работу («майнинг»).

Проблемы применения блокчейна

- Атака Сивиллы - как избежать влияния на сеть злонамеренных участников, регистрирующих множество псевдонимов?
  - Proof-алгоритмы:
    - Proof of Work – очень дорогое удовольствие, не работает в малых масштабах;
    - Proof of Stake – есть фундаментальные проблемы («атака из глубины»), нет возможности старта с нуля;
    - Proof of <придумайте сами> - простор для фантазии.
- Стоимость транзакций
  - вознаграждение валидаторам за поддержку работы сети.
- Скорость транзакций
  - «закапывание» транзакций для гарантии выживания текущей ветви блокчейна.
- Объем хранимых данных
  - Растет с каждой транзакцией

Консорциум (закрытый блокчейн)

- В определенных случаях оказывается выгодно пожертвовать анонимностью, открытостью и бездоверительностью, и получить:
  - Proof of Authority – очень дешевый алгоритм подтверждения;
  - Сложность нахождения блоков можно регулировать до минимальной, при этом распределять право на генерацию блока по оговоренному алгоритму;
  - Стоимость транзакции нулевая, т.к. участники работают не за вознаграждение (не нужна их стимуляция);
  - Глубокое «закапывание» транзакций не является обязательным;
  - Объем данных в некоторых случаях можно уменьшить, храня данные в чистом виде вне блокчейна, и сохраняя в чейне лишь хэш, подтверждающих их существование.

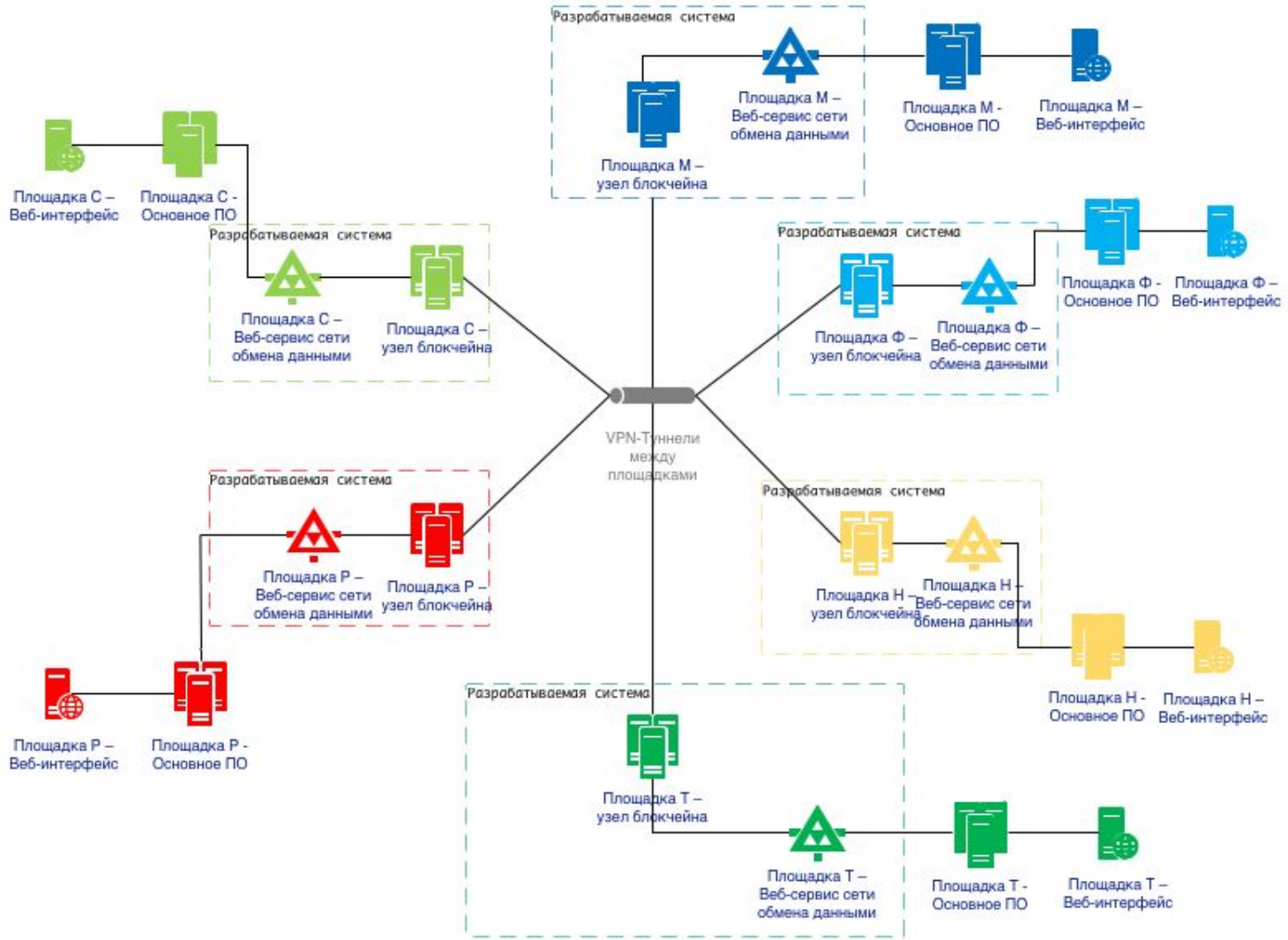
Постановка исходной задачи

- Задача - организация обмена данными между ЭТП, являющимися конкурентами, но нуждающимися в разделении KYC-данных заказчиков для повышения эффективности бизнеса.
- Вопрос доверия:
  - Для централизованной системы все участники должны доверять разработчику и оператору этой системы
  - Обычно приводит к введению в систему какого-либо внешнего арбитра (в лице государства, например).
- Решение - разработать систему децентрализованного хранения KYC данных, позволяющую организовать надежный и безопасный обмен данными без введения в систему единого центра доверия.

Решение задачи с помощью блокчейна

- Применение блокчейна обеспечивает:
  - отсутствие единого центра, которому остальные участники вынуждены доверять;
  - невозможность фальсификации или удаления данных ни одним из участников системы;
  - отсутствие единой точки отказа;
  - распределенный характер системы позволяет любому участнику временно отключаться от системы и продолжать работать с имеющимися данными автономно, а после восстановления подключения – синхронизировать состояние с другими участниками;
  - транзакционный подход к хранению данных позволяет отследить информацию об изменениях каждого элемента данных и позволяет получить все прошлые версии каждого элемента.

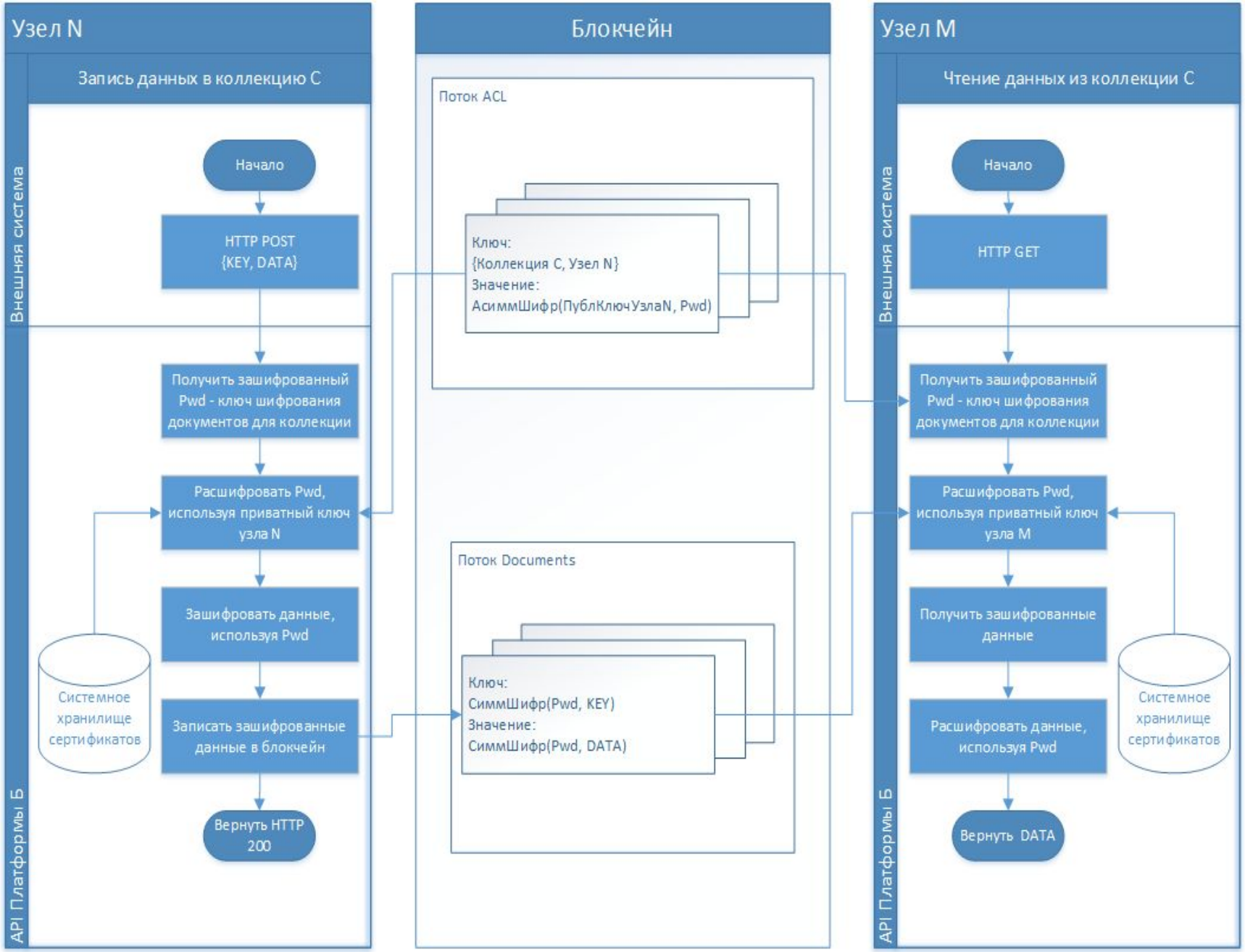
Решение задачи



Возможности разграничения доступа к данным

- Данные могут публиковаться как в виде публично доступного набора данных, так и в виде набора данных с ограниченным доступом;
- Для разграничения доступа к данным система использует криптографическую защиту с помощью ГОСТовских алгоритмов (на основе сертифицированного средства криптозащиты от компании КриптоПро).
- Управлять уровнем доступа и доступностью набора данных для конкретных участников может только создатель этого набора – никаких административных ролей, имеющих полный доступ к данным в системе нет и быть не может;

Гибридное шифрование данных



Реализация решения

- Для реализации блокчейна использована платформа Multichain:
  - Развитая поддержка режима консорциума;
  - Концепция потоков данных;
- Криптозащита на базе Крипто Про CSP
  - Гибридное шифрование данных;
  - Обмен открытыми ключами через блокчейн;
- API, реализующее REST-интерфейс документ-ориентированного хранилища на платформе Microsoft .NET
  - Концепции Коллекции документов (схема валидации, права доступа) и Документа;
  - Поддержка push и pull моделей работы с хранилищем.
- Обобщенное решение, применимое в различных областях.

Ключевые особенности Платформы Б как хранилища данных

- Отсутствие единой точки отказа и единого центра, которому остальные участники вынуждены доверять;
- Невозможность фальсификации или удаления данных, если участник однажды получил к ним доступ;
- Возможность автономной работы и последующей синхронизации данных при подключении к сети;
- Возможность управления доступом к данным, реализованная не через ограничение прав доступа, а через криптозащиту данных с помощью сертифицированных средств криптозащиты;
- Управление уровнем доступа и доступностью набора данных для конкретных участников только со стороны владельца данных;
- Сохранение всей информации об изменениях каждого элемента данных и возможность получения всех прошлых версий каждого элемента;
- Наличие механизма уведомления подписчиков об изменениях данных.

Текущее и будущее применение Платформы Б

- Текущее применение
  - Обмен данными между ЭТП компаний группы Финтендер (РТС-Тендер).
  - На сегодня в продакшне:
    - ~1.5 млн записей за ~полгода эксплуатации
    - ~10 тысяч новых записей в день
- Обсуждаемые сегодня возможности применения:
  - Другие ЭТП
    - Реализация Единой Платформы обмена данными между ЭТП;
    - Whitelabel-лицензирование решения;
  - Операторы ЭДО;
  - Медицинская сфера
    - проект в области клинических испытаний лекарственных препаратов;
    - проект в области управления ЭМК

Потенциальные области применения

- Платформа Б применима для хранения:
  - медицинских данных пациентов;
  - реестров прав собственности и нотариата;
  - логистических данных;
  - любых других защищенных распределенных реестров;
- Ограничения:
  - Необходимость авторизации узлов консорциума (невозможность анонимности);
  - Пропускная способность ограничивается необходимостью шифрования (на практике – порядка нескольких десятков транзакций в секунду);
  - Весь объем хранимых данных дублируется между узлами.

Вопросы?

Всеволод Пелипас

- v.pelipas@solarl.ru
- +7 978 812 07 33
- Skype: pelipas

ООО СоларЛаб

- office@solarl.ru
- +7 978 126 46 24
- г. Севастополь

ул.Брестская 18Б, офис 505

SolarLab>_