Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Построение архитектуры финансовых сервисов на блокчейн. Практика эксплуатации Мастерчейн

Алексей Цветков,
Руководитель группы разработки, Ассоциация «ФинТех»

Ассоциация развития финансовых технологий

Создаём технологические решения, которые содействуют развитию финансового рынка Российской Федерации:

- программное обеспечение, стандарты и протоколы
- предложения по созданию и изменению законодательства в области цифровой экономики

ФИНТЕХ АССОЦИАЦИЯ

Банк России · ГАЗПРОМБАНК · НСПК · ВТБ · открытие БАНК · QIWI · СБЕРБАНК · Тинькофф Банк · Ак Барс Банк · РоссельхозБанк · Альфа-Банк · Райффайзен БАНК

Мастерчейн

Платформа распределенных реестров для финансовых институтов, сертифицирована ФСБ и соответствует требованиям Банка России.

На базе ГОСТ-криптографии реализованы:

- протокол вызова смарт-контрактов Ethereum
- сервис передачи конфиденциальных сообщений
- создание закрытых сетей с управляемым доступом
- средства мониторинга и администрирования

Приложения на Платформе

Взаимодействие участников сети Мастерчейн происходит по единым для всех правилам, фиксируемым в реестре.

Пилотные и промышленные кейсы:

- регистрация и учёт ценных бумаг (закладные)
- торговое финансирование (гарантии, аккредитивы)
- передача платёжной информации

Средства построения приложений

Программный код и результаты выполнения смарт-контрактов в сети Мастерчейн имеют доступность, целостность и неотказуемость.

Как оператор сети мы требуем использовать в прикладных контрактах разработанные нами механизмы отключения и обновления кода.

```
// Контракт с возможностью отключения
contract Suspendable {

    // Флаг отключения
    bool public disabled;

    // Барьер: отключен ли контракт?
    modifier enabled() {
        require(disabled == false);
        _;
    }
    // Функция проверки прав администратора,
    // реализуется в дочерних контрактах
    function canDisable()
    public view returns(bool);

    // Отключить для изменения
```

```
// Контракт с возможностью обновления
contract Upgradable is Suspendable {

    // Адрес предыдущей версии
    Upgradable public precursor;

    // Адрес следующей версии
    Upgradable public successor;

    // Инициализировать с указанием
    // адреса предыдущей версии
    function Upgradable(Upgradable _precursor)
    public {
        if (_precursor != address(0))
            _precursor.upgradeWith(this);
        precursor = _precursor;
    }
```

```
    // Указать адрес следующей версии
    // и отключить
    function upgradeWith(Upgradable _successor)
    public {
        disable();
        successor = _successor;
    }

    // Название смарт-контракта
    function contractName()
    public pure returns(string);

    // Версия смарт-контракта
    function contractVersion()
    public pure returns(string);

}
```

Приложения для финансового сектора

Техническая задача: обеспечить безопасность взаимодействия.

Участники Ассоциации и другие финансовые институты:

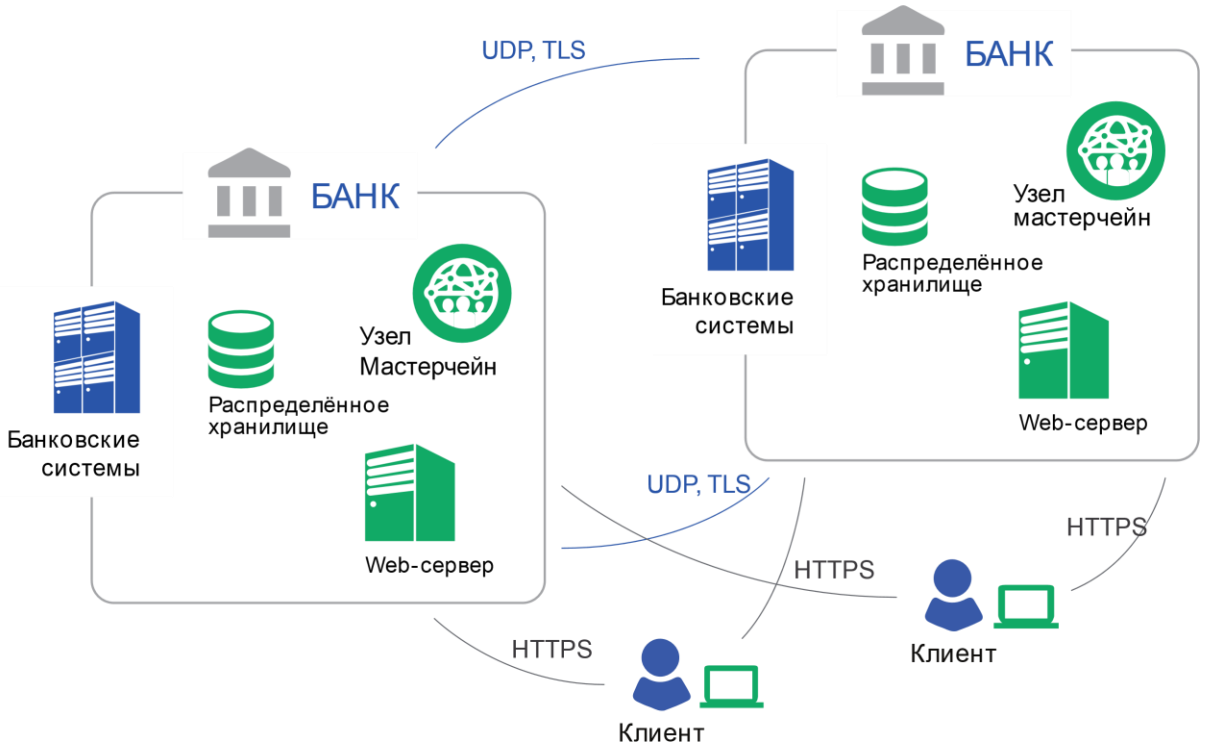
- самостоятельно управляют своей инфраструктурой
- строят бизнес-процессы обособленно

Зрелость процессов обеспечения безопасности сильно различается между организациями.

Применимость традиционного решения

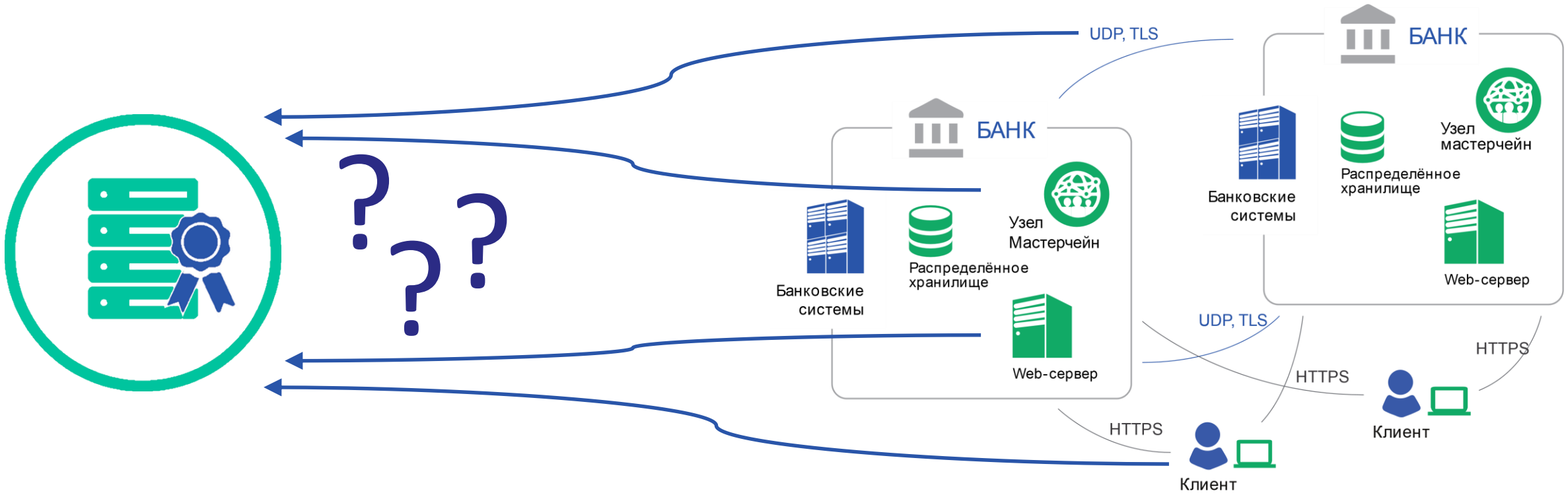
Системы распределённых реестров позволяют объединить ресурсы каждого участника в доверенную цифровую среду.

Для согласованного управления криптографическими операциями и для проверки их результатов используется PKI.

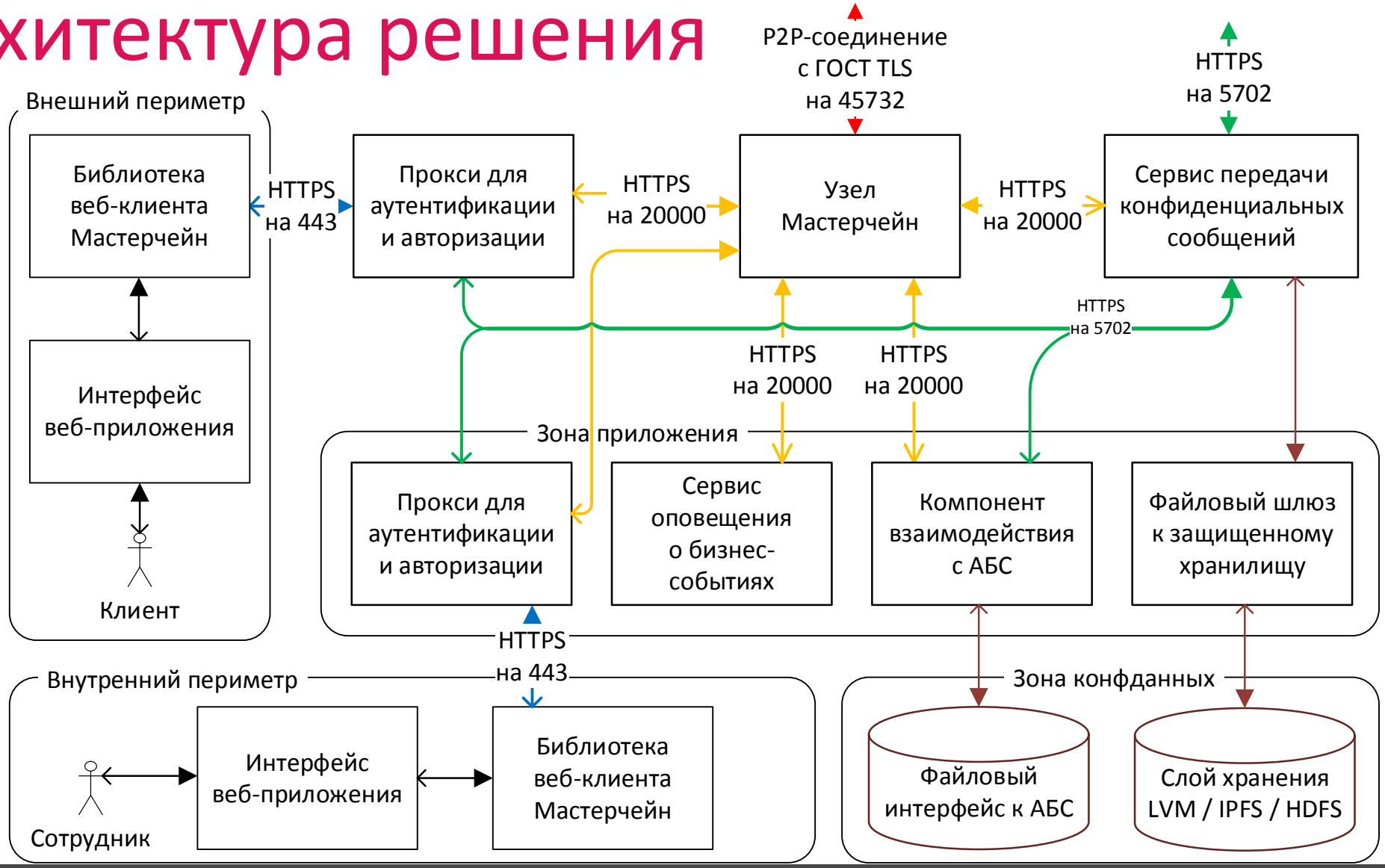


Специфика распределённых реестров

В среде распределённых реестров PKI должна быть встроена так, чтобы сохранить отказоустойчивость и производительность.



Архитектура решения



Сочетание PKI и бизнес-логики приложений

Внедрение PKI в логику бизнес-процессов осложняется,

так как необходимо заменять ключи с течением времени.

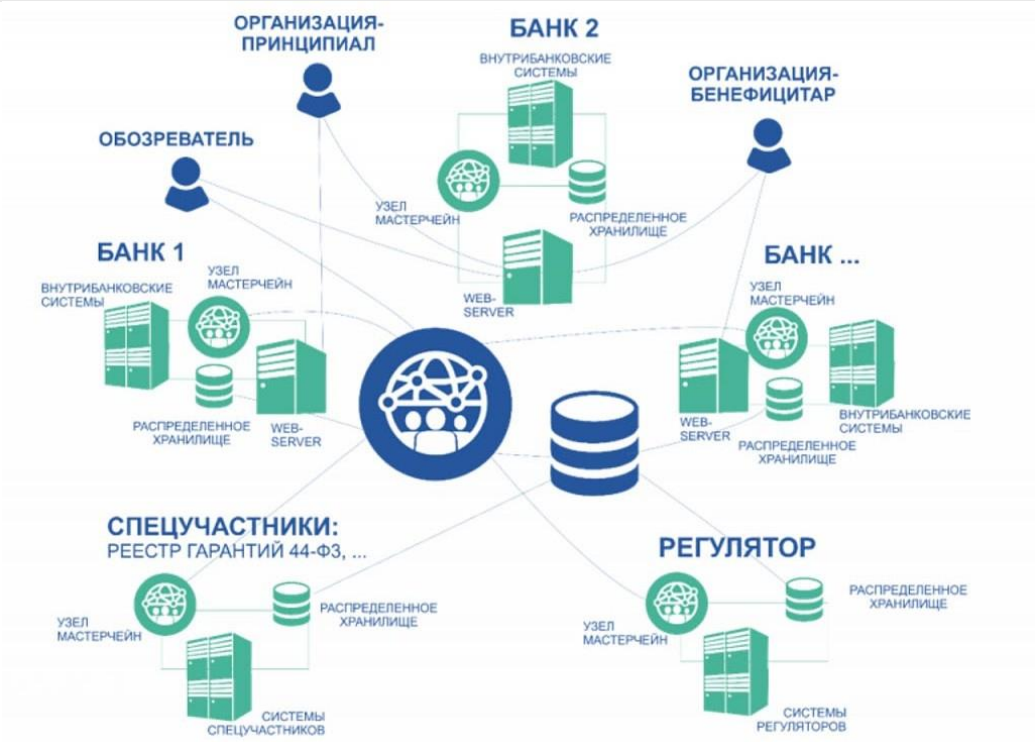
Авторизация бизнес-операций

должна происходить на основании

отношений между организациями.

Структура отношений в кейсе

может быть многоуровневой.



Сертификаты раздельного назначения

Оператор сети является оператором распределённого КриптоПро УЦ 2.0.

Он управляет выпуском и отзывом сертификатов участников сети.

В шаблоны выпускаемых сертификатов добавлены OID для разделения ключей по типам операций в разделе 1.2.643.6.57.1:

1.1.1 [TLS Server] Узел Мастерчейн	2.1.1 [TLS Server] API СПКС	5.1.1 [TLS Server] API ИС
1.1.2 [TLS Client] Узел Мастерчейн	2.1.2 [TLS Client] API СПКС	5.1.2 [TLS Client] API ИС
1.1.3 [TLS Server] API узла Мастерчейн	2.2.1 [Sign] Узел СПКС	5.1.3 [TLS Client] АРМ ИС
1.3.1 [Sign] Узел Мастерчейн	2.4.1 [Encryption] Хранилище СПКС	5.2.1 [Sign] АРМ ИС Админ АФТ
3.1.3 [TLS Client] АРМ Админ сети	2.4.2 [Encryption] Робот ИС	5.2.2 [Sign] АРМ ИС Робот
3.2.1 [Sign] Админ сети АФТ	2.4.3 [Encryption] Менеджер ИС	5.2.3 [Sign] АРМ ИС Админ
3.2.2 [Sign] Админ Whitelist		5.2.4 [Sign] АРМ ИС Менеджер

Расширенная схема электронной подписи

Цели и причины использования: совместимость с протоколом Ethereum, сокращение объёма хранимой и передаваемой информации

Смарт-контракт реестра Мастерчейн

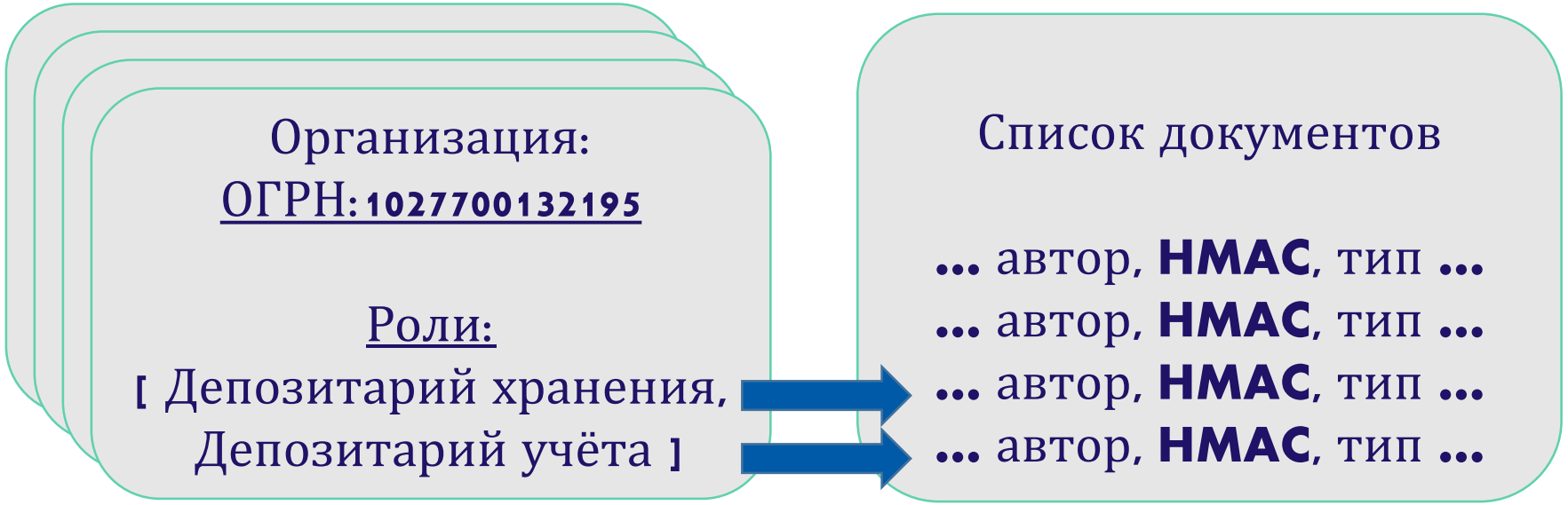
В системном контракте в блокчейне перечислены:

- веб-сервисы сети (узлы) с указанием организации-владельца
- организации участники-сети с перечислением их сертификатов
- сертификаты X.509 и назначенные им должностные полномочия

Смарт-контракт бизнес-процесса

Каждая сделка в блокчейне представлена перечислением:

- организаций-участников и их ролей в процессе
- конфиденциальных документов (сертификат автора, HMAC, тип, …)



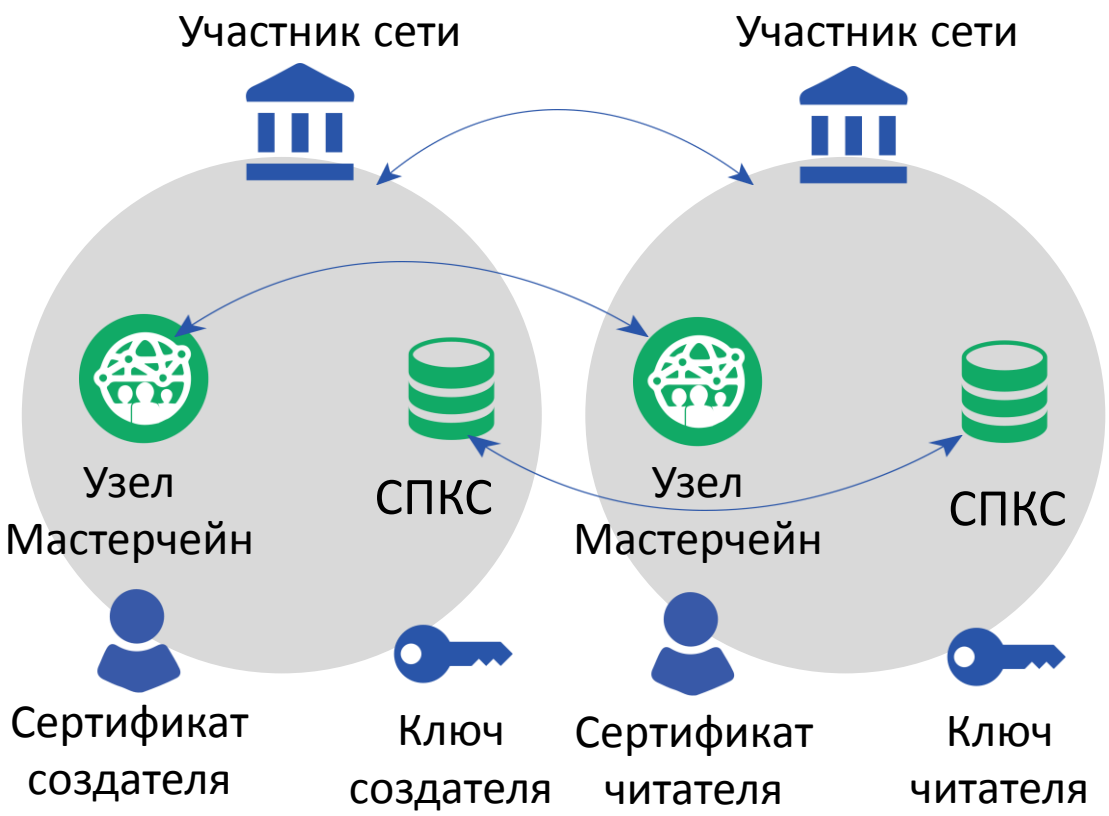
Смарт-контракт ролевой модели

Разработчик приложения записывает матрицу прав доступа в контракт.

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Чтение	Ипотечная закладная	Менеджер	[Депозитарий хранения]
Запись	Черновик гарантии	Операционист	[Банк-гарант]
Чтение	Документ-основание	*Все сотрудники*	[*Все участники сделки*]
Запись	Назначение полномочий	Администратор	[Оператор сети]

Передача конфиденциальных сообщений

Веб-сервис предоставляет доступ к документам согласно ролевой модели.

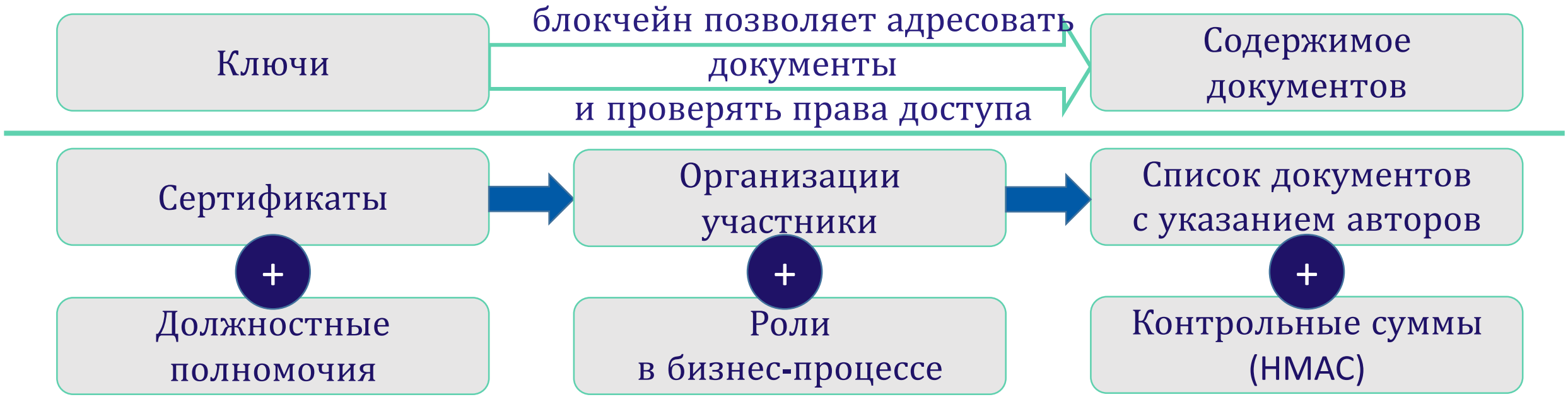


1. Аутентификация запросов и ответов производится по сертификатам.
2. В реестре публикуются события о сохранении документов на узлах.
3. Читатель по записи в реестре находит узел и запрашивает документ.
4. Копию документа читатель сохраняет на своём узле сети.

Ролевая модель Мастерчейн

Системные смарт-контракты платформы обеспечивают:

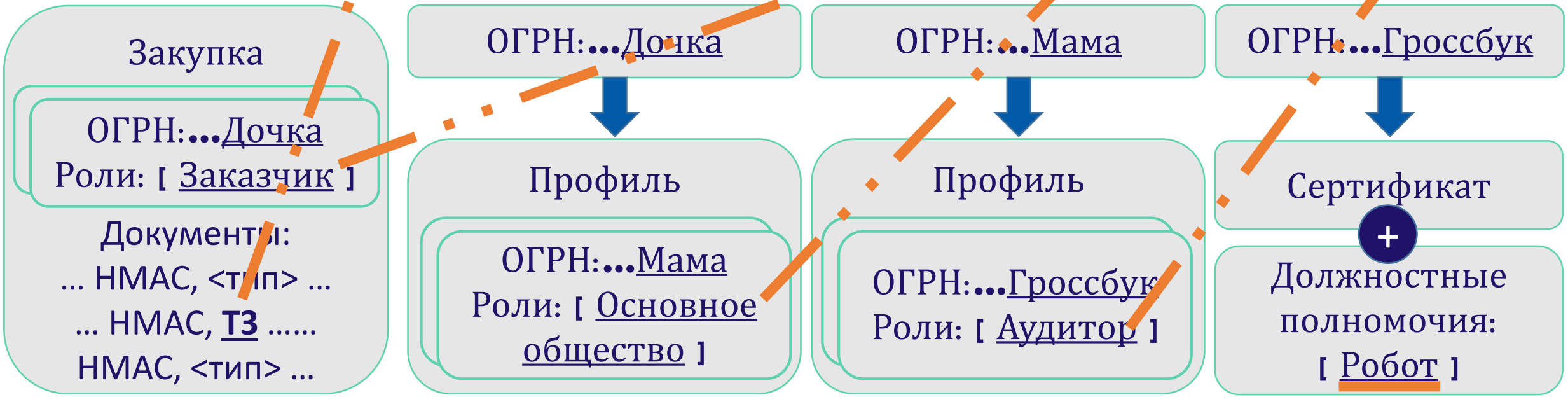
- независимость бизнес-процессов от процесса управления ключами
- конфиденциальность документов, их целостность и неотказуемость



Многоуровневая ролевая модель

В матрице прав доступа возможно указать последовательность ролей.

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Чтение	Техническое задание	Робот	[Заказчик, Основное общество, Аудитор]



Примеры ролевых моделей

Прямое дебетование (разрешение на списание оплаты за услуги).

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Запись	Платёж	Робот	[Владелец, Поставщик услуг]
Чтение	Платёж	Робот	[Банк]
Запись	Баланс	Робот	[Банк]

ОГРН:...Банк В

Сертификат

+

Должностные полномочия:
[Робот]

Счёт

Банк В: [Банк]

АФТ: [Владелец]

... HMAC, **Баланс** ...
... HMAC, **Платёж** ...

ОГРН:...АФТ

Профиль

Телеком:
[Поставщик услуг]

ОГРН:...Телеком

Сертификат

+

Должностные полномочия:
[Робот]

Примеры ролевых моделей

Закрытый факторинг (с уведомлением в случае невыплаты).

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Запись	Универсальный передаточный документ	Директор	[Продавец]
Чтение	Универсальный передаточный документ	Робот	[Продавец, Фактор]
Запись	Уведомление об уступке	Робот	[Продавец, Фактор]

Покупка

Телеком: [Продавец]

АФТ: [Покупатель]

… HMAC, **УПД** …
… HMAC, <тип> …
… HMAC, **УОУ** …

ОГРН:…Телеком

Профиль

Банк Р: [Фактор]

ОГРН:…Банк Р

Сертификат

+

Должностные полномочия:
[Робот]

Примеры ролевых моделей

Управление реестром участников сети как бизнес-процесс.

Права	Тип объекта доступа	Полномочия ключа	Роли организаций
Запись	Регистрация сервисов	Администратор	[Оператор]
Запись	Регистрация организаций-клиентов	Администратор	[Банк]
Запись	Назначение полномочий сертификата	Администратор	[Клиент]

Смарт-контракт реестра Мастерчейн наследует контракт бизнес-процесса.

Проверки прав на изменения реестра выполняются согласно ролевой модели.

Приложения могут определять новые типы объектов и проверять права доступа к ним в своих смарт-контрактах или веб-сервисах.

Результаты

Мастерчейн полноценно использует и расширяет концепцию PKI.

Средства платформы позволяют повысить доступность и удобство использования сертификатов.

Ролевая модель и средства администрирования позволяют отделить управление сертификатами ключей от бизнес-логики.

Дополнительные механизмы авторизации реализованы в виде программного кода в распределённом реестре.

Ассоциация «ФинТех»

Алексей Цветков,

руководитель группы разработки,

направление распределённых реестров

E-mail: alexey.tsvetkov@fintechru.org

Telegram: @aitsvet

Сайт: https://fintechru.org