#partadfintech

ПИЛОТНЫЕ ПРОЕКТЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ РБД/БЛОКЧЕЙН В УЧЕТНОЙ ИНФРАСТРУКТУРЕ

Ярославль 2018

Fintech

ПАРТАД

Децентрализованное хранилище сертификатов ключей электронных подписей клиентов финансовых институтов

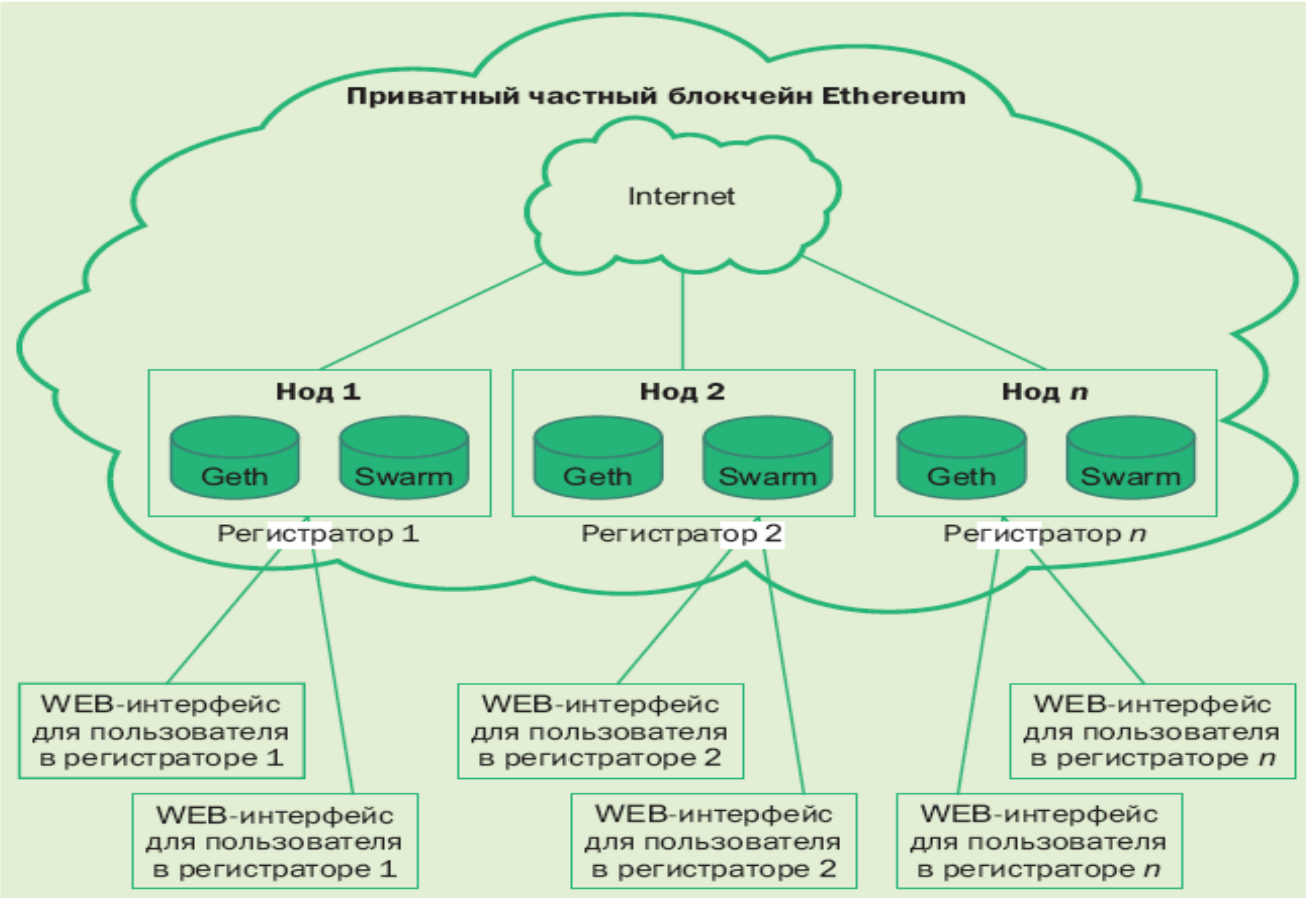
#partadfintech

- Развернуты приватный частный блокчейн Ethereum с использованием алгоритма Proof of Authority (право на запись имеет только идентифицировавший себя узел) и распределенная система хранения файлов SWARM. Блокчейн построен по принципу консорциума, т.е. предназначен для ограниченного круга лиц (участников проекта), которые знают друг друга (не анонимны). Администратором смарт-контракта, дающего доступ к распределенному хранилищу сертификатов, является ЦУС ПАРТАД.

- Смарт-контракт описывает сущности как сертификата ключа, так и всех участников проекта, что позволяет на уровне программного кода администрировать доступ к данным. В смарт-контракте хранится следующая информация: данные об удостоверяющем центре издавшем сертификат ключа электронной подписи, данные о владельце сертификата, хэш сертификата в файловом хранилище SWARM, а также данные участника сети, загрузившего данный сертификат.

Децентрализованное хранилище сертификатов ключей электронных подписей клиентов финансовых институтов

#partadfintech



Распределенная база данных электронных профилей клиентов участников финансового рынка

#partadfintech

➢При разработке данного смарт-контракта, обеспечивающего формирование электронного профиля клиента участника финансового рынка (владелец паев – физическое лицо):

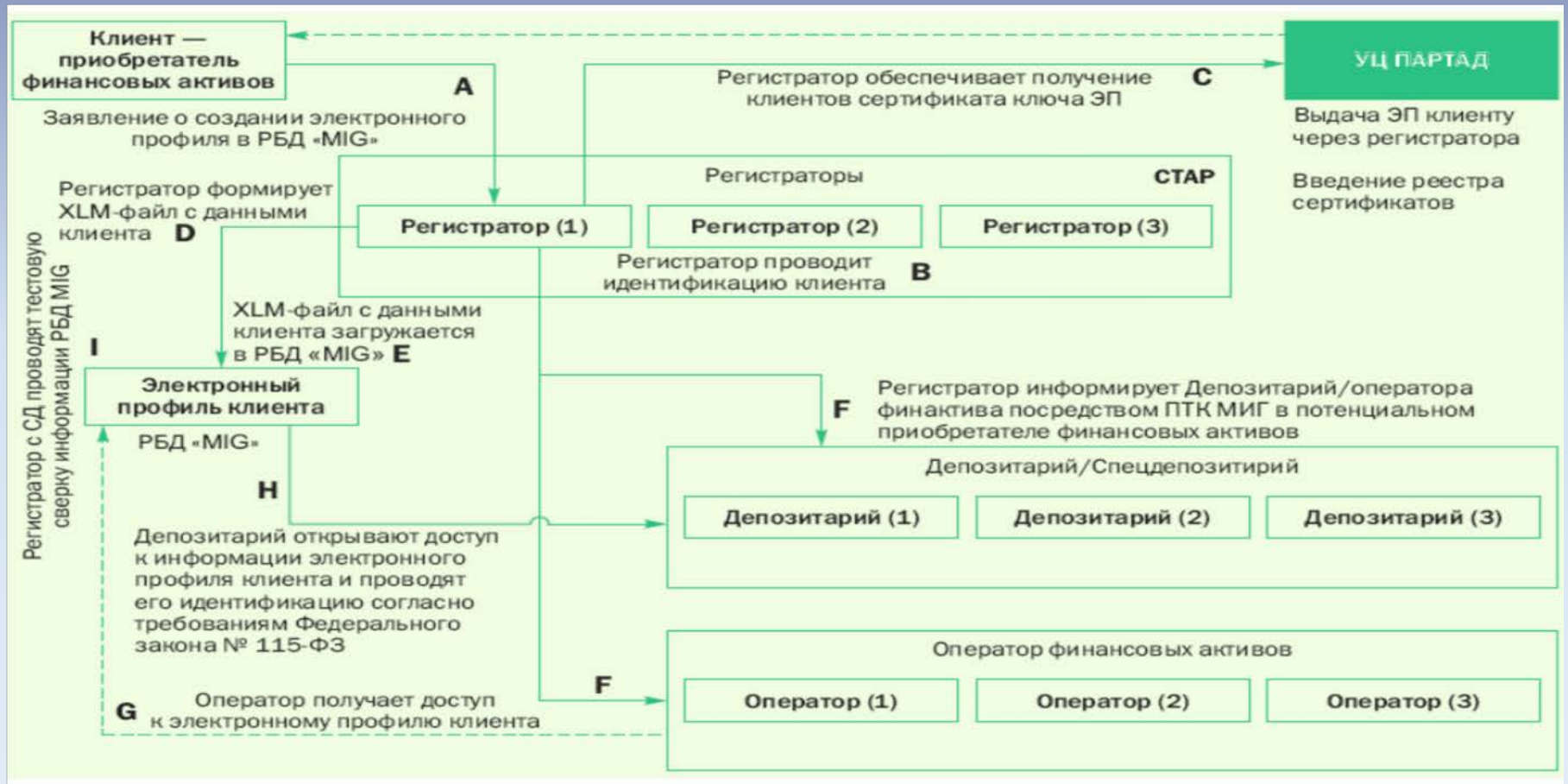
✓используются XML-форматы.

✓учитывается сценарий тестирования распределенной сети в целях формирования электронного профиля лица — владельца финансовых активов.

✓реализуется шифрование XML-файлов электронного профиля перед загрузкой в SWARM во избежание несанкционированного доступа к данным электронного профиля участника финансового рынка.

Распределенная база данных электронных профилей клиентов участников финансового рынка

#partadfintech



Распределенная база данных электронных профилей клиентов участников финансового рынка

#partadfintech

Основные особенности пилотного проекта электронного профиля

- **Реализуется офф-лайн подписание транзакций. Закрытый ключ находится не на НОДе а рядом с приложением, что позволяет подписывать транзакцию локально и отправлять на любую НОДу сети.**

- **Используется более сложная структура администрирования пользователей (администратор смарт-контракта, администратор участников, участник).**

- **Каждый профиль участника финансового рынка это отдельный смарт-контракт создаваемый автоматически при загрузке профиля в блокчейн. Позволяет вести историю версий (изменений) файла электронного профиля и ограничивать доступ к этим данным.**

ВЫВОДЫ

Преимущества блокчейна

- легкость проверки целостности базы данных.
- каждое изменение в системе имеет свою временную метку.
- резервное копирование в режиме реального времени.
- аудит учетной системы в режиме реального времени.

Недостатки (ограничения) блокчейна

- обладает меньшей пропускной способностью, чем система с одним центром управления. Внесение изменений требует больше времени.
- хранение избыточного объема данных. Каждый, кто участвует в управлении такой системой, должен иметь у себя копию базы данных, которая постоянно обновляется.
- распределенная ответственность.