

TAXNET

Построение ЭДО на основе технологии «блокчейн»

Предпосылки и подводные камни

Закиев Ренат

Блокчейн - текущее состояние

- Новая технология (относительно)
- Попытки применить в различных сферах
- Различные подходы к созданию систем
- Несформировавшаяся область исследований
- Высокий интерес и повышенные ожидания

Блокчейн - текущее состояние

TAXNET

”

Блокчейн
– это машина
по воспроизводству
доверия.

”

Эта мода
навязана
методами маркетинга

”

С блокчейн-технологией,
Интернет приобретает
новый уровень функциональности

Блокчейн-экосистема

TAXNET

Мировую блокчейн-экосистему можно условно разделить на три класса:

1

Децентрализованные автономные организации и приложения, такие как Bitcoin, Ethereum, BitShares и др.

2

Блокчейн-сервисы

3

Приватные блокчейн-системы

Блокчейн - текущее состояние

TAXNET

Мы рассматриваем ее именно как технологию, а не модель бизнеса или заработка!

Блокчейн - это система, которая представляет собой децентрализованную базу данных. Эта база содержит информацию о всех транзакциях, когда-либо проведенных участниками системы.

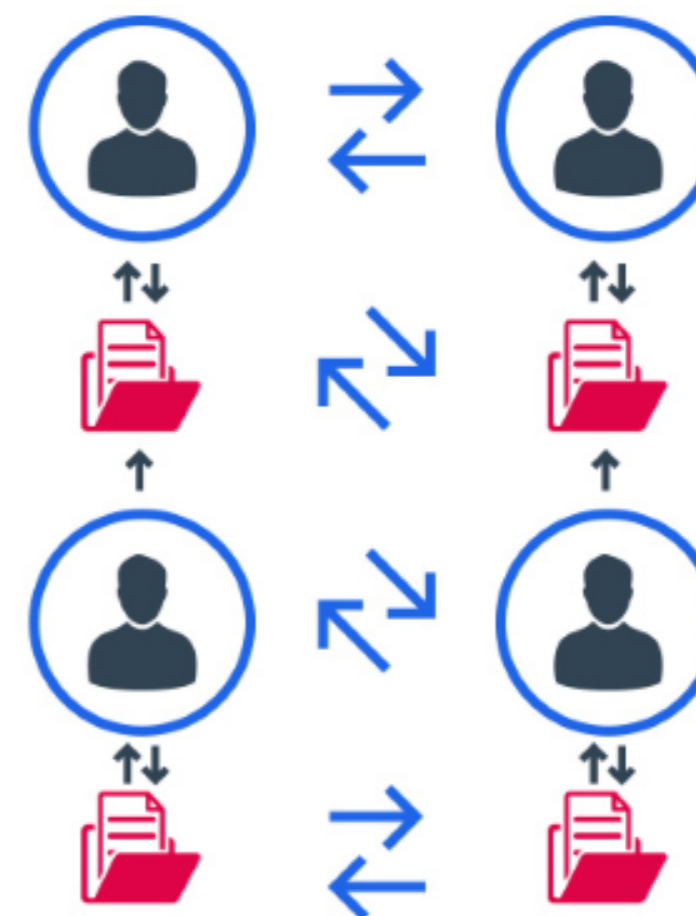
Простыми словами

Блокчейн - это публичный реестр всех осуществленных в системе операций, который сосредоточен не в одном месте, а распределен между всеми пользователями системы.

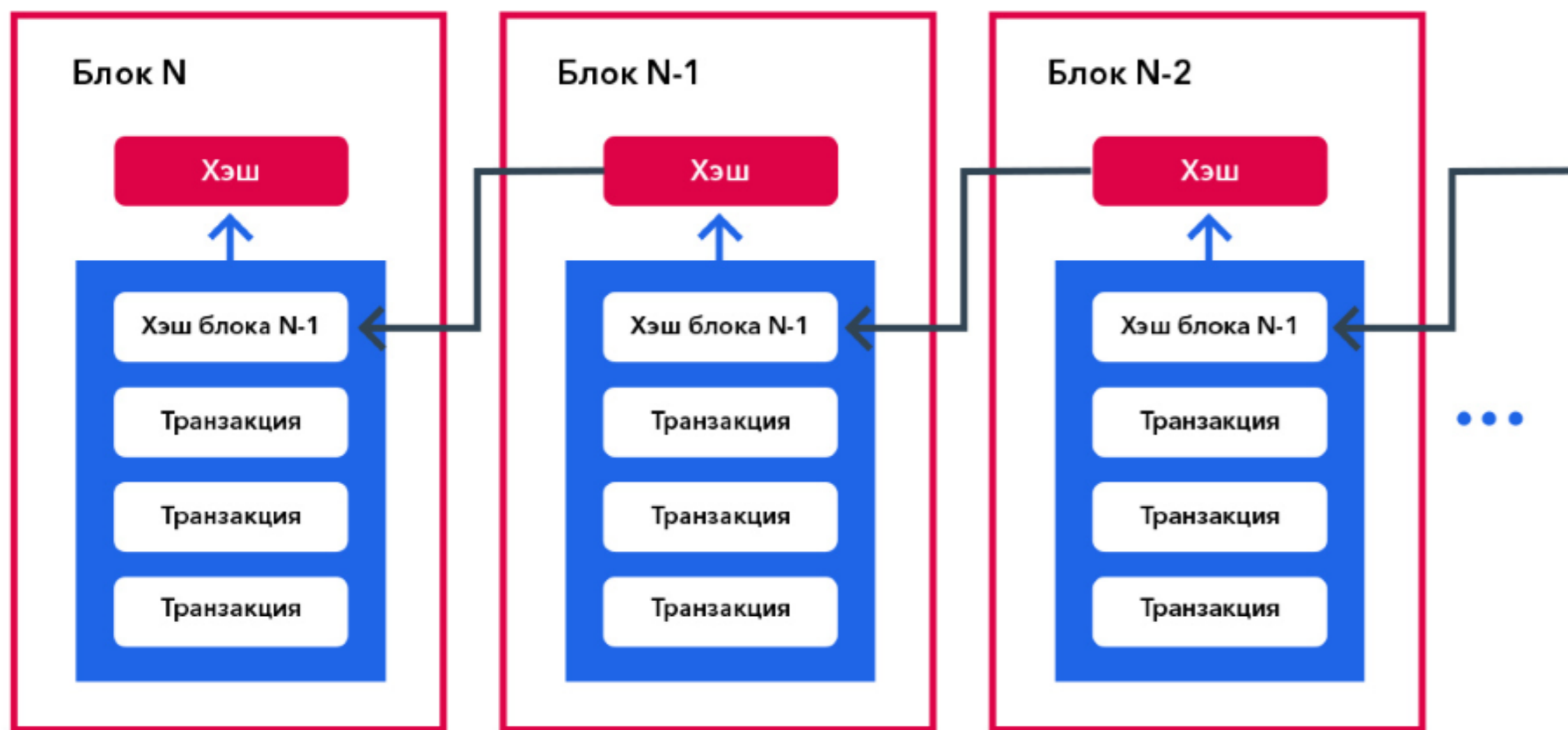
Централизованная сеть



Децентрализованная сеть



Блокчейн - текущее состояние



- Сеть, состоящая из компьютеров, хранящих реестр транзакций
- Есть два ключа (приватный/публичный)
- Транзакция, которую можно проверить
- Каждая транзакция связывается с предыдущей

Блокчейн - основные принципы

TAXNET

Распределенность

Данные хранятся у всех пользователей сети/платформы. Не требуется создание какого-либо централизованного дата-центра

Открытость

Данные о транзакциях могут быть видны всем участникам процесса/системы

Защищенность

Однажды сделанную запись невозможно подделать или удалить. Данные о каждой транзакции защищены шифрованием, а также ключами доступа.

Независимость

Благодаря устройству сети пользователи не нуждаются в никаких посредниках

Блокчейн - текущее состояние

TAXNET

С технической точки зрения, блокчейн возможно применять везде, где необходимо:

- 1 обеспечить распределенность и анонимность операций
- 2 с одновременным обеспечением высокого уровня безопасности
- 3 без необходимости участия в операциях третьей



Электронный документооборот на блокчейне?

Задача

Удовлетворение серьезной потребности бизнеса в сфере документооборота

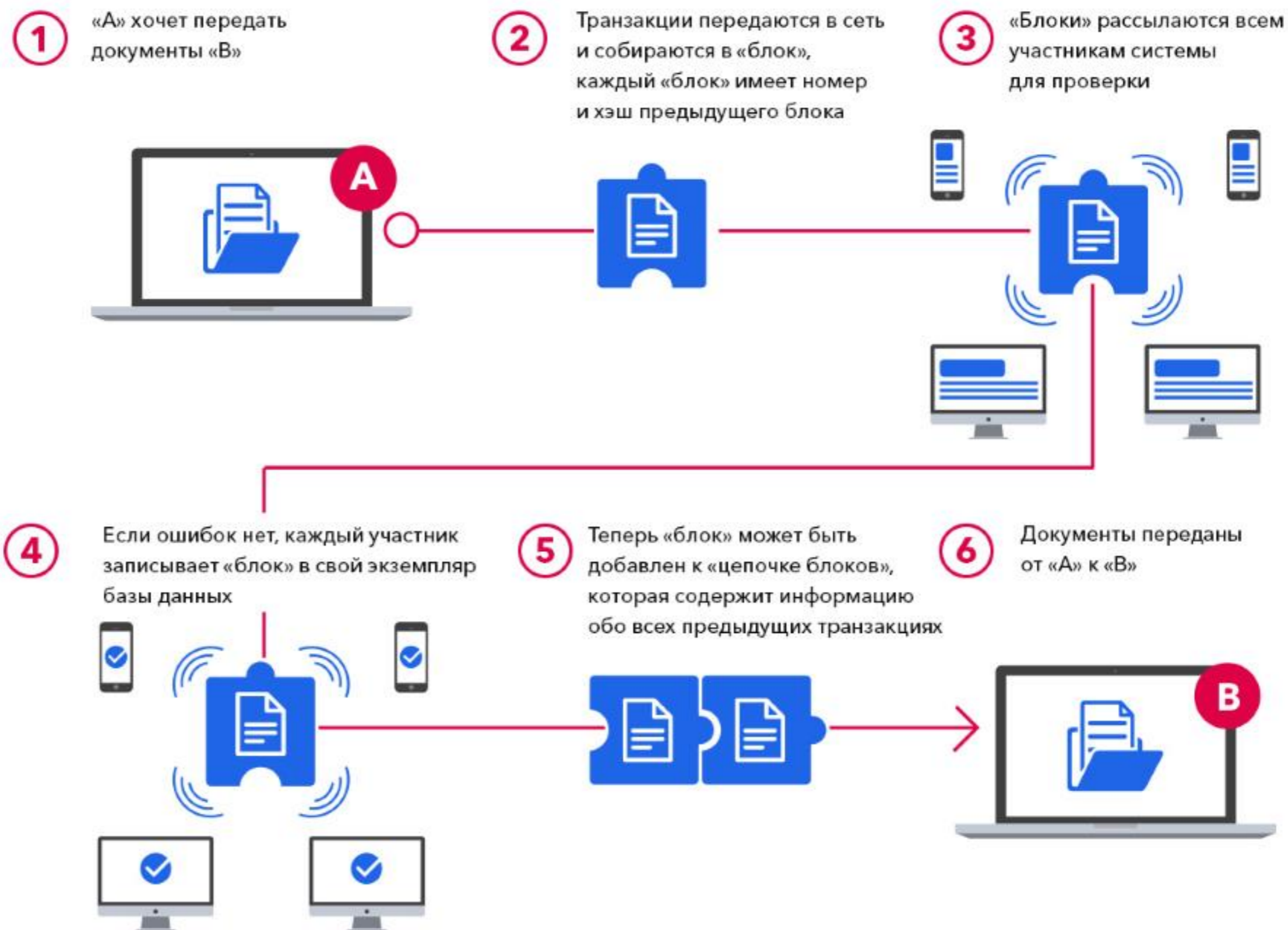


- упрощение процессов и обеспечение правовой безопасности
- максимально надежное хранение документов, предотвращение их потери, защита от подделок и злоупотреблений
- дать возможность себе и третьим лицам верифицировать бумажные документы по цифровым оригиналам, которые подделать невозможно

ЭДО на Блокчейн. Проект Z

TAXNET

Как работает блокчейн



ЭДО на Блокчейн. Проект Z

TAXNET

- Изучаем ГОСТ Стандарт 34.11-2012, которые описывают алгоритм хэширования данных (вместо Ethash, SHA, MD5)
- Система, реализующая интерфейс обмена данными и средства разграничения доступа к данным, разработана на платформе .NET.
- Используется закрытый блокчейн (консорциум) - т.е. для подключения к нему требуется согласование узлом-координатором
- Система не предусматривает удаления данных, таким образом, ни один участник не может удалить документ, доступный другим участникам.
- При обновлении документа, сохраняется полная история его изменений, и есть возможность получения любой из версий документа.
- Система имеет API, изолирующий пользователя от деталей реализации самого блокчейна и позволяющий работать с понятиями более высокого уровня «документ»

Z - как сервис для текущих систем ЭДО

TAXNET

Проверка достоверности документов через блокчейн

Создается хэш документов, переданных на рассмотрение через СЭД и сохраняется в блокчейн-цепочках эфириума.

Используется API (интерфейс программирования приложений) RESTful.

Когда хеш находится в общей блокчейн цепочке, документ невозможно изменить без аннулирования хэша - гарантия как конфиденциальности документа, так и доступности данных для проверки достоверности.



ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ
ТРАНСКРИПТ

Z - как сервис для текущих систем ЭДО

TAXNET

Подпись документов
с помощью



Sign



Пользователь создает свою собственную уникальную цифровую подпись с помощью функционала сайта. Затем загружает на сайт и подписывает его.

При необходимости тот же документ могут подписывать и другие люди



56V268
673351

Подписанный документ преобразуется в 32-х значный цифровой и буквенный ряд



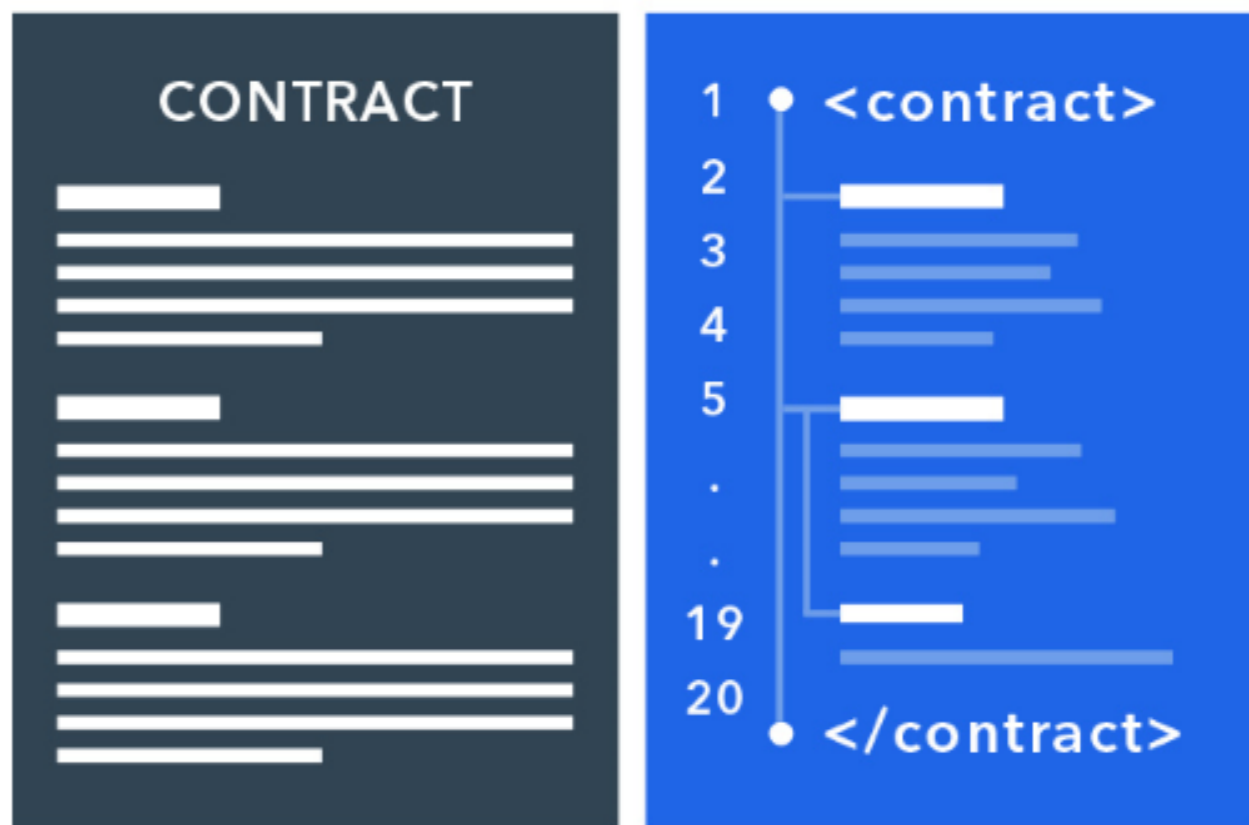
Этот цифровой ряд записывается в блокчейн Биткойна, посредством транзакции в сети с адреса, привязанного к аккаунту пользователя на Z-Sign. Таким образом, легко проверить, кто именно подписал конкретный документ

Смарт-контракты

Смарт-контракты – это специально созданные алгоритмы, которые запускаются самостоятельно при выполнении определенных условий.

Смарт-контракт может обновить данные в блокчейне в соответствии с изначально заданными правилами.

Гибкий самоконтролируемый документооборот между контрагентами.



Смарт-контракт хранится в распределительном реестре и ни одна из сторон не способна его заменить или переделать.

Блокчейн и подводные камни

TAXNET



Низкая скорость работы из-за криптографии (Ethereum протокол Ghost - повышенная скорость транзакций)



Настройка и управление инфраструктурой



Отсутствие надежных и эффективных технологических решений



Отсутствие правового поля, юридическая значимость записей в блокчейне

Перспективы

TAXNET

Самая большая проблема на сегодняшний день - **управление.**

Все разногласия, которые ведутся вокруг блокчейна - это вопросы управления и контроля!

- Законодательное регулирование
- Обоснование эффективности и безопасности систем, использующих блокчейн
- Идентификация/аутентификация/авторизация
- Доверенные криптографические методы обеспечения безопасности в таких системах



– Спасибо!

renat-z@taxnet.ru