PKI и блокчейн как технологическая основа цифровых активов

Владимир Комисаренко, заместитель директора по развитию проектов в сфере защиты информации

LWO

Применение технологии блокчейн стабилизировалось

- нереалистичные ожидания, ажиотаж прошли
- все заинтересованные разобрались, и кто счел целесообразным - реализовали соответствующие внедрения
- около 92 % из блокчейн-проектов потерпели неудачу

Основное применение

- Криптовалюты, как тип цифрового токена (99%)
- Цифровые токены, кроме криптовалют (1%)

Платформы для создания и управления токенами

- ERC-20
- NFT
- другие

Интернет активов

- Это не только криптовалюты. Все, чем вы можете владеть, может быть представлено, продано и использовано в качестве невзаимозаменяемых токенов (non-fungible tokens, NFT)
- Вы можете токенизировать свое искусство и автоматически получать гонорары при каждой перепродаже. Или используйте токен для того, что у вас есть, чтобы взять ссуду
- Возможности постоянно растут

NFT

- NFT отличаются от токенов ERC-20 тем, что каждый отдельный токен полностью уникален и не делится
- NFT дают возможность назначать или заявлять право собственности на любую уникальную часть цифровых данных, отслеживаемых с помощью блокчейна
- NFT создается из цифровых объектов как представление цифровых или нецифровых активов

NFT может представлять

Цифровое искусство:

- Гифки
- Музыка
- Видео

Предметы реального мира:

- Документы на машину
- Билеты на мероприятие в реальном мире
- Токенизированные счета
- Документы

Детали

- NFT может быть только один владелец
- Право собственности управляется с помощью уникального идентификатора и метаданных, которые не может воспроизвести ни один другой токен
- NFT создаются с помощью смарт-контрактов, которые передают право собственности и управляют возможностью передачи NFT
- При создании выполняет код, хранящийся в смарт-контрактах. Эта информация добавляется в цепочку блоков, в которой осуществляется управление NFT
- Жизненный цикл: создание нового блока, подтверждение информации, запись информации в блокчейн

Экология

Борьба за экологичность – перевод блокчейн на другие принципы (существенно менее энергозатратные, основанные на доверии к независимым вычислителям)

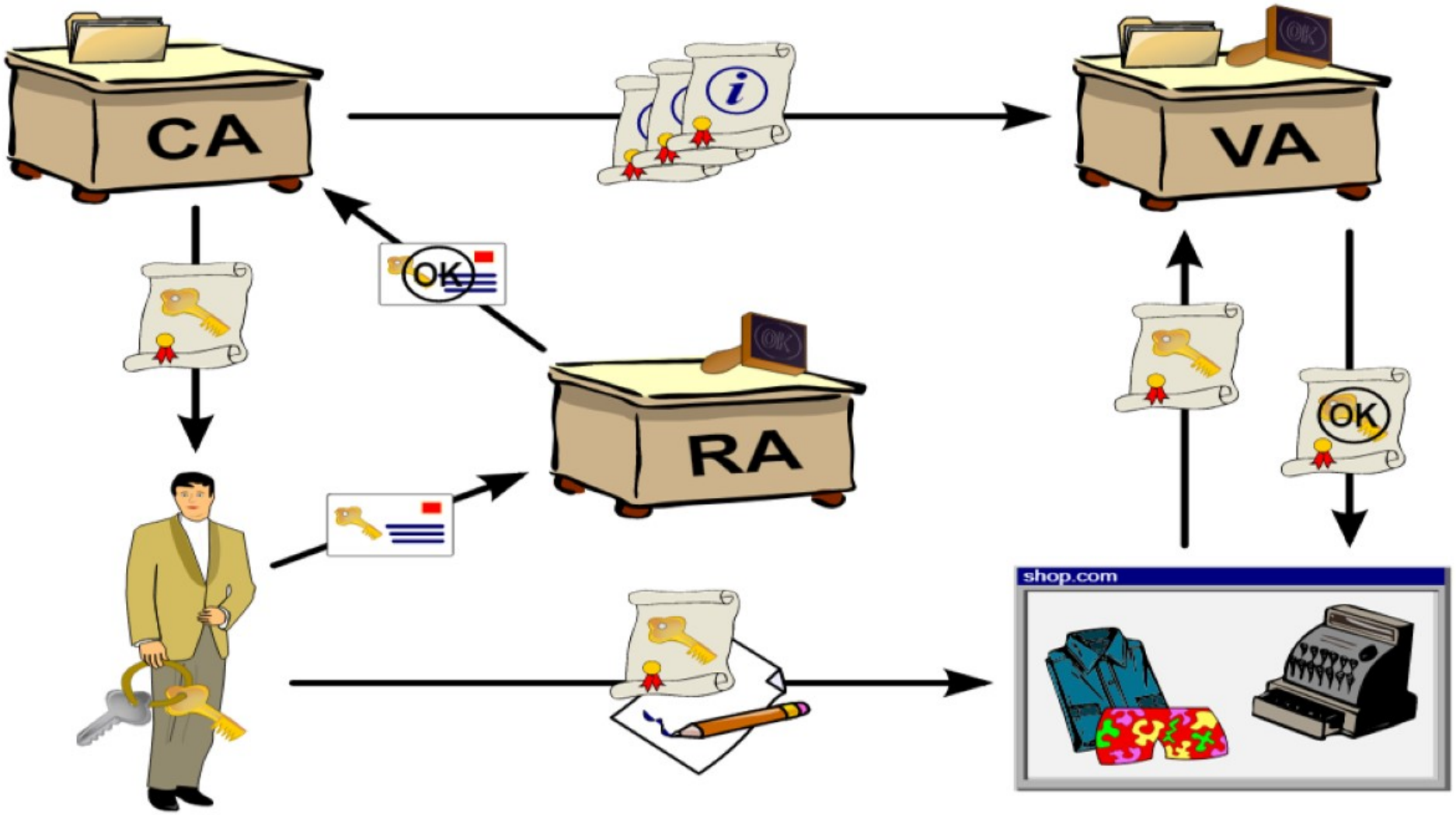
Токен, как подписанный электронный документ

Их значимость зависимости от:

- используемых алгоритмов электронной подписи
- программ электронной подписи
- безопасности применения:

  - доверия открытым ключам проверки подписи,
  - защиты ключей подписи,
  - защиты от атак через среду исполнения программ электронной подписи

PKI



259-ФЗ «О цифровых финансовых активах, цифровой валюте … »

- … выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы
- цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые … … обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам

259-ФЗ «О цифровых финансовых активах, цифровой валюте … »

- под распределенным реестром понимается совокупность баз данных, тождественность содержащейся информации в которых обеспечивается на основе установленных алгоритмов (алгоритма)
- под узлами информационной системы понимаются пользователи информационной системы на основе распределенного реестра, обеспечивающие тождественность информации, содержащейся в указанной информационной системе, с использованием процедур подтверждения действительности вносимых в нее (изменяемых в ней) записей

259-ФЗ «О цифровых финансовых активах, цифровой валюте … »

- **Решение о выпуске цифровых финансовых активов составляется в электронной форме и должно быть подписано усиленной квалифицированной электронной подписью индивидуального предпринимателя, выпускающего цифровые финансовые активы, или усиленной квалифицированной электронной подписью (усиленными квалифицированными электронными подписями) лица (лиц) …**

LWO

В ритме инноваций

lwo.by
contact@lwo.by
+375 17 334 10 02
+375 17 334 28 27
ул. Кропоткина, д. 91, Минск
Республика Беларусь, 220002