

СТАНДАРТЫ ТОКЕНОВ СЕТИ ETHEREUM И ИХ ОСОБЕННОСТИ В РЕАЛИЗАЦИИ РАБОТЫ СМАРТ-КОНТРАКТОВ

Набешко Г. А., Захарьев В. А.

Кафедра систем управления, кафедра защиты информации, Белорусский государственный университет информатики и радиоэлектроники

Минск, Республика Беларусь

E-mail: gnabeshko@gmail.com, zahariev@bsuir.by

Данная статья посвящена исследованию стандартов токенов сети Ethereum. В ней представлена информация о наиболее популярных видах токенов, подробно рассмотрены ключевые особенности в реализации работы смарт-контрактов для каждого вида токена, приведен сравнительный анализ.

ВВЕДЕНИЕ

Реестр блоков транзакций (блокчейн) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

Блокчейн — это, по существу, распределённая база данных или публичная книга всех транзакций или цифровых событий, которые были выполнены и распределены между участвующими сторонами в одноранговых сетях.

Токен — это единица учёта, не являющаяся криптовалютой, предназначенная для представления цифрового баланса в некотором активе, иными словами — выполняющая функцию «заменителя ценных бумаг» в цифровом мире.

Технологически токены реализуются на базе некоторой блокчейн платформы, обеспечивающей возможность записи в распределённый реестр блоков балансов токенов и транзакций. В настоящее время основной платформой для создания токенов является Ethereum.

I. СМАРТ-КОНТРАКТЫ

Смарт-контракт (англ. Smart contract — умный контракт) — компьютерный алгоритм, предназначенный для формирования, контроля и предоставления информации о владении чем-либо. Чаще всего речь идет о применении технологии блокчейна. В более узком смысле под смарт-контрактом понимается набор функций и данных (текущее состояние), находящихся по определённому адресу в блокчейне.

Базовые принципы смарт-контрактов уже были реализованы в блокчейне Биткойна, но их возможности были сильно ограничены и не подходили для того, чтобы создавать на их основе токены для отдельных распределённых приложений. Именно по этой причине можно считать, что Ethereum является первой платформой, которая полноценно развила идею смарт-контрактов и внедрила ее в работу.

Основная идея работы смарт-контракта заключается в следующем: когда вы проводите

транзакцию, отправляя токены на адрес получателя, на самом деле отправляется инструкция в смарт-контракт о том, что у данного количества монет сменился адрес владельца. Именно в результате данного действия у отправителя токены пропадают, а у получателя появляются.

Внутри смарт-контракта можно прописать уникальную механику токена. Он будет работать, но другие разработчики (и смарт-контракты) не смогут обращаться к нему с помощью универсальной логики.

На помощь приходят стандарты. Т.к. Ethereum является open-source проектом (кстати, ERC — это Ethereum Request for Comments), логично, что новый стандарт токена может предложить любой пользователь. Если стандарт решает какую-то важную проблему, то он может стать официальным стандартом Ethereum. Все ERC формализуются в виде EIP (Ethereum Improvement Proposal/предложения по улучшению сети Ethereum).

В настоящее время на веб-странице Ethereum EIP имеется более 150 EIP, при этом часто появляются и новые. Мы рассмотрим 5 самых популярных EIP:

- ERC20 — Смарт-контракт ICO;
- ERC223 — Предотвращает отправку токенов некорректному адресату;
- ERC721 — Не взаимозаменяемые токены;
- ERC777 — Новый расширенный стандарт токена;
- ERC1155 — Стандарт мульти-токена.

II. СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ ЦИФРОВЫХ ТОКЕНОВ

1. ERC20 Standard — смарт-контракт ICO
Стандарт ERC20 является самым популярным для ICO. Стандарт ERC-20 определяет набор правил, которые должны быть соблюдены для того, чтобы токен был принят и имел возможность взаимодействовать с другими токенами в сети.

Сценарии использования токенов ERC-20 самые различные. Например, они могут выступать как акции проекта, сертификаты, подтвер-

ждающие владение активами, очки в программах лояльности или как криптовалюта.

Преимущества использования ERC-20:

- Упрощается листинг на криптовалютных биржах;
- Улучшается взаимодействие с разными сетями;
- Аудит смарт-контрактов становится более предсказуем и стандартизирован;
- Становится легче создавать и поддерживать пользовательские инструменты и кошельки, вокруг экосистемы Ethereum.

Стандарт ERC-20 предусматривает шесть обязательных функций для любого смарт-контракта.

Функции:

Total Supply: Общая эмиссия токенов.

Balance: Изначальное количество токенов.

Allowance: Сумма, которую разрешено снимать с владельца.

Transfer: Передача токена по указанному адресу.

Approve: Позволяет снимать определенное количество токенов с договора.

Transfer From: Передача токенов с источника на адрес.

2. ERC223 Standard – Предотвращает отправку токенов некорректному адресату. ERC223 был предложен Daxagan в декабре 2017 года. Стандарт ERC20 страдает от невозможности обработки входящих транзакций по контракту от получателя. Большая проблема заключается в том, как не предназначенные для адресата токены могут быть отправлены по контракту. Эти средства могут потеряться.

Стандарт ERC223 представляет новую функцию отмены транзакций, которой нет в существующем стандарте ERC20, чтобы предотвратить случайную передачу токенов. Это оптимальное решение, чтобы токены не потерялись в сети Ethereum, что очень важно.

3. ERC721 Standard – Не взаимозаменяемые (non-fungible) токены ERC721 Standard – один из более перспективных ERC-стандартов, который применяется для активно развивающихся не взаимозаменяемых токенов. Не взаимозаменяемыми называются токены, или активы, которые нельзя обменять на другой такой же токен, или актив, в отличие от стандартных эфириума и биткойна. Самые известные из таких токенов – это CryptoKitties.

Следующий стандарт позволяет реализовать стандартный API для не взаимозаменяемых токенов (NFT) в смарт-контрактах. Этот стандарт обеспечивает базовый функционал для отслеживания и передачи NFT. Они могут представлять права собственности на цифровые или физические активы.

4. ERC777 – новый расширенный стандарт токена. Этот стандарт определяет новый способ взаимодействия с контрактами по токенам, оставаясь полностью совместимым с ERC20.

Особенности:

- Стандарт позволяет использовать одну транзакцию для работы со смарт-контрактами вместо двух при обмене одного токена на другой;
- Соблюдение процедур AML/KYC;
- Возможность отклонить передачу и получение токена;
- Держатели токенов могут разрешать/запрещать передачу токенов другими операторами от их лица;
- Дополнительное поле для свободных сообщений-комментариев.

5. ERC1155 – Стандарт мульти-токена

Идею этого стандарта предложили разработчики проекта Enjin в 2018. Enjin – проект, стремящийся к упрощению создания игр на Ethereum.

Особенности:

- Позволяет выпускать несколько токенов в одном контракте;
- Токены в одном контракте могут быть fungible и non-fungible одновременно;
- Поддерживает атомарные свопы;
- Поддерживает «batch» транзакции;
- Не для всех транзакций нужно ждать окончания блока.

III. СПИСОК ЛИТЕРАТУРЫ

1. Ethereum Improvement Proposals [Электронный ресурс]. – Режим доступа: <https://eips.ethereum.org/erc>.
2. Википедия [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki>.
3. GitHub. Ethereum Improvement Proposals [Электронный ресурс]. – Режим доступа: <https://github.com/ethereum/EIPs>.
4. Introducing Ethereum and Solidity / Dannen, Chris // Apress – 2017.