IS4302
Blockchain and Distributed Ledger Technology

Lecture 3
27 Jan, 2023

NUS
National University
of Singapore

Overview

- **Important standards of Ethereum**

Important standards

- **ERC165 – method introspection**
- **ERC820#/1820 – contract registry**
- **Token standards:**
  - ERC20
  - ERC721 – Non-fungible token
  - ERC777 – improved ERC20
  - ERC998 – composable NFT
  - EIP1155/EIP1178*/EIP1203* – Multi-class token (FT or NFT class)
- **ERC137/181 – ethereum domain name service**
- **EIP1078* – universal login**
- **ERC1776** – meta transactions**
- **ERC1337** – subscription payment**

#obsolete
*draft
**early proposal

ERC20

- **Simple API to simulate a token using a smart contract. Allow anyone to easily create a new token.**
  - totalSupply()
  - balanceOf(address _owner)
  - transfer(address _to, uint256 _value)
  - transferFrom(address _from, address _to, uint256 _value)
  - approve(address _spender, uint256 _value)
  - allowance(address _owner, address _spender)

ERC721 (Non-fungible token)

- **fungibility - property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.**
- **Non-fungible token – represent something unique**
  - Eg. Cryptokitty DNA, tagged physical asset

ERC721 (Non-fungible token)

- **Main difference to ERC-20:**
  - `function ownerOf(uint256 _tokenId) returns (address)`
  - `function safeTransferFrom(address _from, address _to, uint256 _tokenId)`
  - `function transferFrom(address _from, address _to, uint256 _tokenId)`
- **`uint256`** identifier for each unique token (vs just a ‘balance’ in ERC-20)

ERC721 (Non-fungible token)

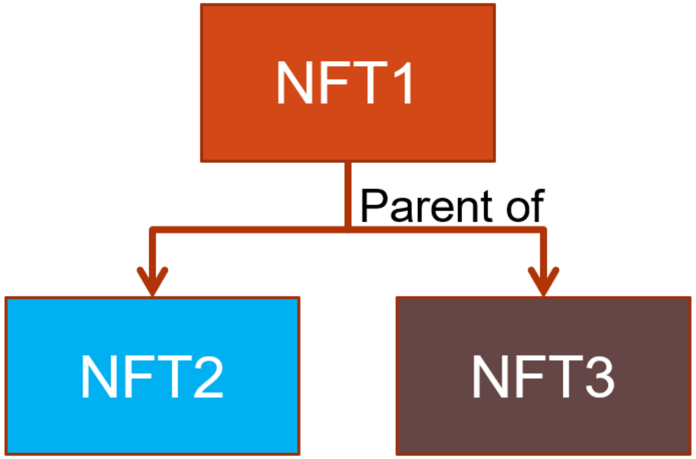
- **safe version of transfer performs a supportsInterface() check before transfer (ERC-165)**

- **Previously, many <u>token ‘lost’ due to erroneous transfer </u>to contract address, which has no way to ‘use’ token properly**

ERC998 (Composable NFT)

- **ERC721 as a ‘tree’**
- **Allow for child → parent, parent → child**
- **Transferring asset as a tree/subtree**

- **Use case:**
  - Bundle of game asset
  - Bundle of physically connected asset



ERC1155/1178*/1203*(Multi-class token)

- **Multiclass fungible token**
- **Main difference to ERC20, ERC721:**
  - `function safeTransferFrom(address _from, address _to, uint256 _id, uint256 _value, bytes calldata _data) external`
  - `uint256` identifier for each token class
  - `uint256` value for each token class

ERC1155/1178*/1203*(Multi-class token)

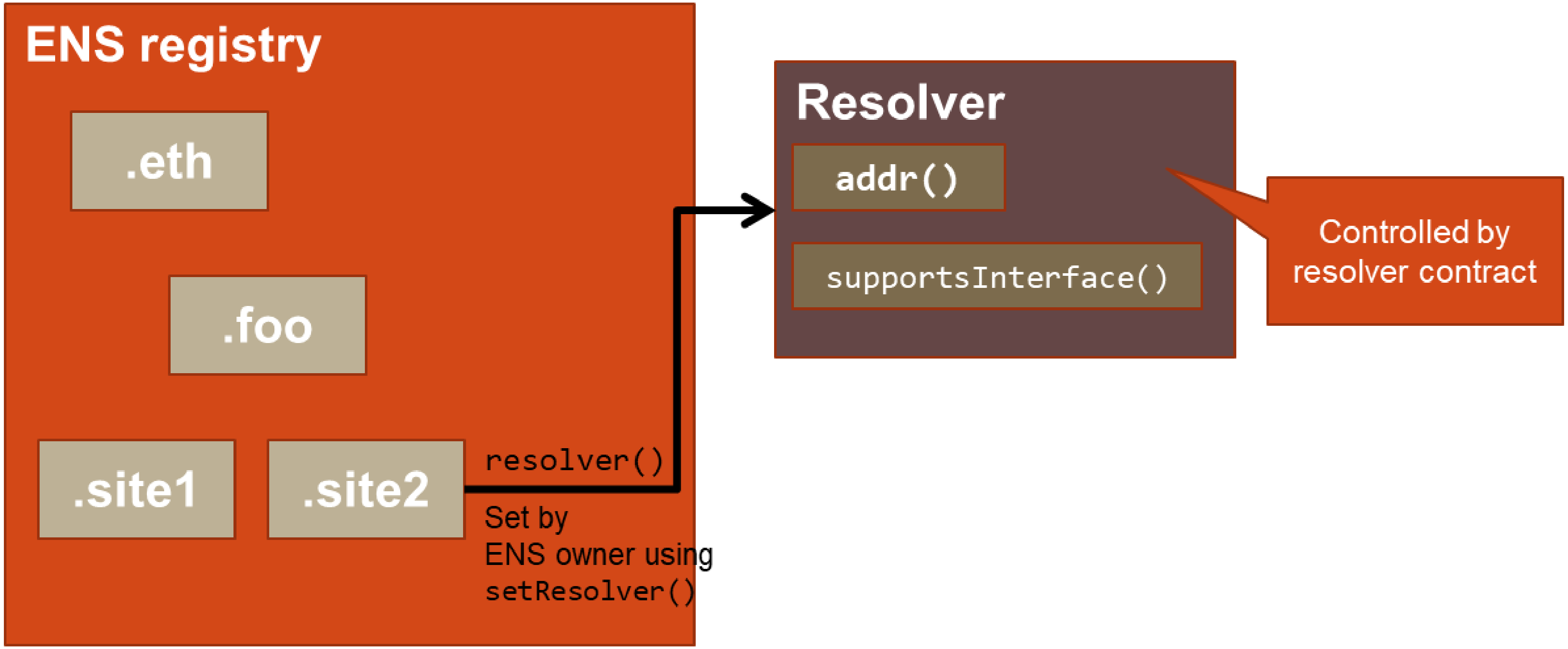
- **Safe version of transfer which performs a supportsInterface() check before transfer (ERC-165)**

- **`function safeBatchTransferFrom(address _from, address _to, uint256[] calldata _ids, uint256[] calldata _values, bytes calldata _data) external`**

Ethereum name service (ENS)

- **Allow for decentralized naming service (similar to DNS)**
- **ENS registry as a smart contract**
- **Forward(ERC137) and reverse(ERC181) lookup**
- **Referenced using a hash tree**
- **Registry to find 'Resolver' contract – provides information on address and supported interface**
  - ENS owner allowed to change resolve linkage
  - Resolver owner allowed to change address linkage

Ethereum name service (ENS)



ERC1078*(Universal login)

- **Using on-chain identity proxy as a contract (EIP725)**
  - execute arbitrary contract calls

    ```
    function execute(uint256 _operationType, address _to,
    uint256 _value, bytes _data)
    ```

  - hold arbitrary data

    ```
    getData(bytes32 _key), setData (bytes32 _key, bytes _value)
    ```

  - Can act as on-chain owner of all kinds of token
  - Address of proxy using ENS (ERC165)

ERC1078*(Universal login)

- **Having ephemeral handles to proxy contract**
  - Multiple devices as handle to contract
  - Define multi-sig condition
  - Able to define transaction classes / limitations
  - Social recovery (defined social network who can help recover)

- **Remove reliance on single ‘cold’ recovery (user-unfriendly)**

Subscription payment (ERC1337**)

- **Regular subscription payment using smart contract. “Standing order” as smart contract**
  - User defined schedule
  - User able to cancel at any time
  - Helps ensure recurring income for business owners

Thank you!

Reminder:
Lab 2 submission is due 11:59pm next Wednesday
There will be lab sessions before the lecture next week

Slides based on work by Dr Suen Chun Hui