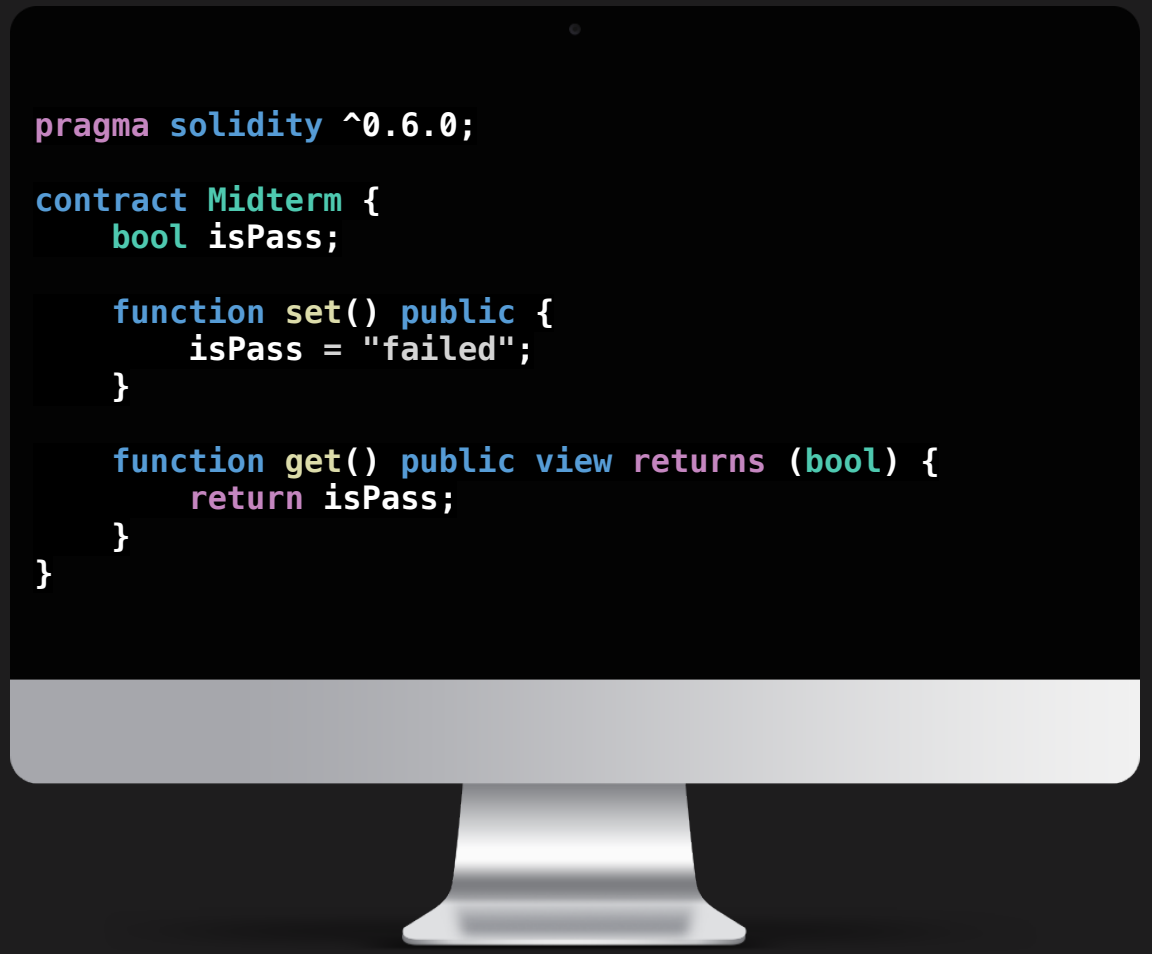
# Smart Contract 3

- 陳博宇 @ 東吳大學 -

# 目錄







# - ERC 20 介紹與實作-

# EIP ( Ethereum Improvement Proposals )



- Standard Track EIP
  - Core - 共識分叉的改進、核心開發相關。( EIP-5 OP Code Gas Price)
  - Networking - 網路協議相關。( EIP-1459 DNS)
  - Interface - client端的規範和標準的改進，或是語言層級的標準。( EIP-1102 )
  - ERC - 應用程式層級相關標準與協定。( EIP-55、EIP-75、EIP-85 )
- Informational EIP
  - 描述以太坊設計的問題，或向以太坊社群提供一般指導或資訊，但不提出新功能。
- Meta EIP
  - 對 Ethereum 的改進或建議。(EIP-1)

EIP

# ERC20



發行總量

```
function totalSupply() external view returns (uint);
```

帳戶 Token 餘額

```
function balanceOf(address tokenOwner) external view returns (uint balance);
```

A 批准給 B 的數量

```
function allowance(address tokenOwner, address spender) external view returns (uint remaining);
```

```
function transfer(address to, uint tokens) external returns (bool success);
```
← 轉移代幣

```
function approve(address spender, uint tokens) external returns (bool success);
```
← 批准自己代幣轉移

```
function transferFrom(address from, address to, uint tokens) external returns (bool success);
```

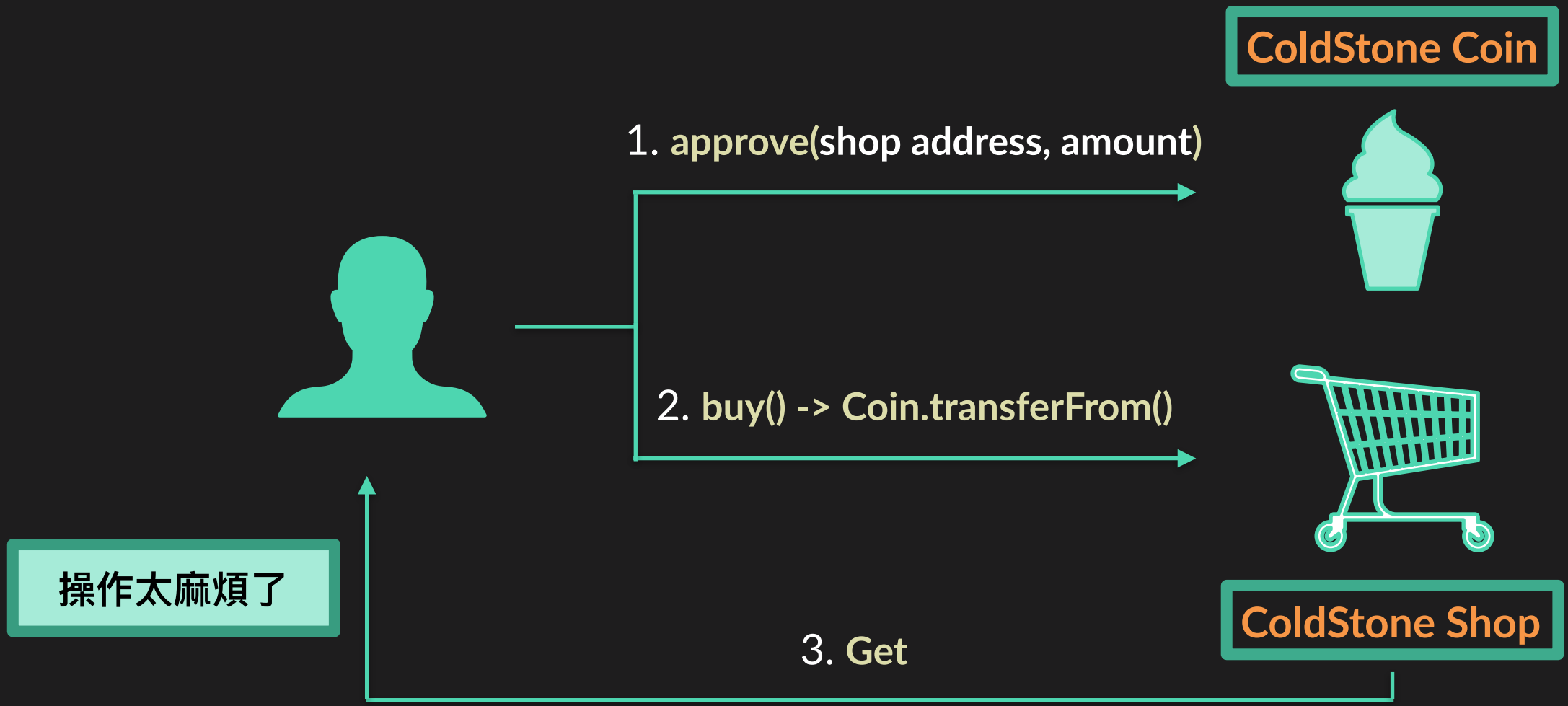
將 A 代幣移轉給 B

```
event Transfer(address indexed from, address indexed to, uint tokens);
```

```
event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
```

# ERC20 - 購物合約示意圖





- 在 Token 合約：

```
function approveAndCall(
    address spender,
    uint tokens,
    bytes memory data
)
    public returns (bool success) {
    approve(spender, tokens);
    ApproveAndCallFallBack(spender).receiveApproval(msg.sender, tokens, address(this), data);
    return true;
}
```

- 在 Shop 合約：

```
function receiveApproval(address _sender, uint256 _value, bytes _extraData){
    require(msg.sender == tokenContract);
    // do something …
}
```

# - ERC 721 介紹與實作-

# ERC721



- Non-Fungible Tokens
- 每個 Token 是獨一無二的
- 不可互換
- 不可分割

# 理解ERC721之前



- ERC165

```
interface ERC165 {
    function supportsInterface(bytes4 interfaceID) external view returns (bool);
}
```

- True when interfaceID is 0x01ffc9a7 (EIP165 interface)
- False when interfaceID is 0xffffffff
- True for any other interfaceID this contract implements
- False for any other interfaceID

# ERC721



額外檢查 to，tokenId的有效性,而且如果 to 是合約地址，會再觸發回掉韓數

```
function balanceOf(address owner) external view returns (uint256 balance);
function ownerOf(uint256 tokenId) external view returns (address owner);
function safeTransferFrom(address from, address to, uint256 tokenId) external;
function transferFrom(address from, address to, uint256 tokenId) external;
function approve(address to, uint256 tokenId) external;
function getApproved(uint256 tokenId) external view returns (address operator);
function setApprovalForAll(address operator, bool _approved) external;
function isApprovedForAll(address owner, address operator) external view returns(bool);
function safeTransferFrom(address from, address to, uint256 tokenId, bytes calldata) external;
event Transfer(address indexed from, address indexed to, uint256 indexed tokenId);
event Approval(address indexed owner, address indexed approved, uint256 indexed tokenId);
event ApprovalForAll(address indexed owner, address indexed operator, bool approved);
```

← 指定地址管理權限

自定義參數

# - 智能合約的隨機數-

# 方便的隨機數



- 好用的block

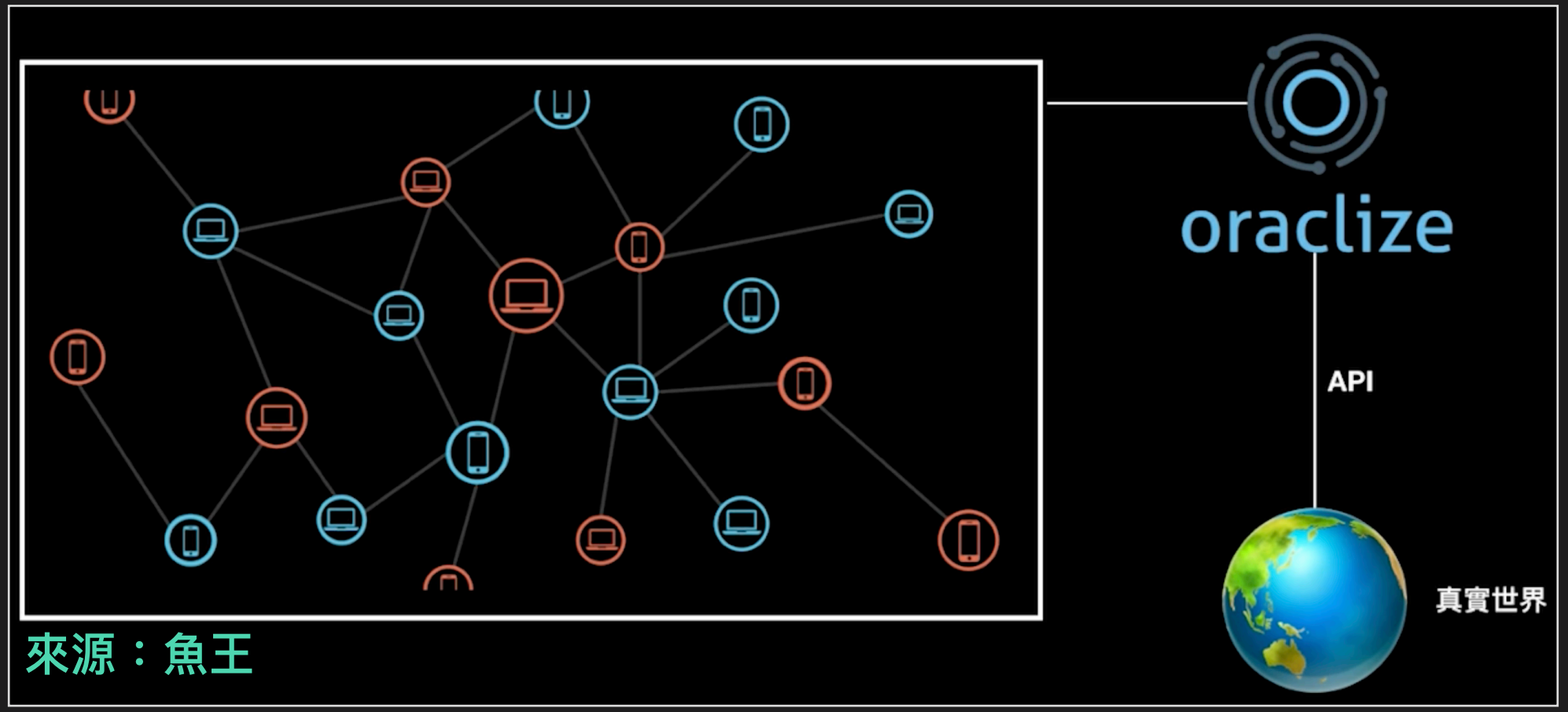
可預測變數？

```
function random() public view returns(uint256) {
    bytes32 result = keccak256(abi.encodePacked(
            block.timestamp,
            blockhash(block.number),
            msg.sender));
    return uint256(result);
}
```

# Oraclize



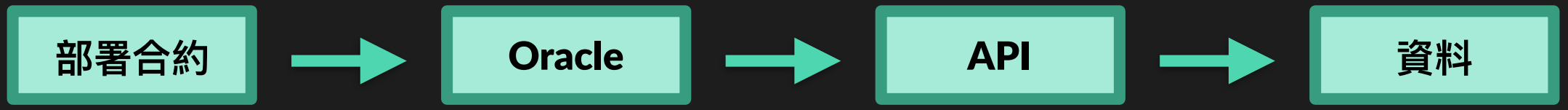
- 要收費
- 串連真實世界




來源：魚王

# Oraclize 流程






Random Number API : https://42bchen.com/randomNum

# - E N D -