



NEP5 Token Standard

NEO Smart Contract

林鹏涛

Peter Lin

区块链 The BlockChain

信任的机器



■ 区块链 The BlockChain

比特币

2008年，中本聪发布了《比特币：一种点对点的电子现金系统》白皮书

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

区块链 The BlockChain

比特币

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘

GENESIS BLOCK

000000000019d6689c085ae165831e934ff
763ae46a2a6c172b3f1b60a8ce26f



■ 区块链 The BlockChain

比特币

去中心化的电子账簿系统

没有中央银行的货币

P2P

密码学

共识机制

... ..

■ 区块链 The BlockChain

信任的机器

区块链让人们在互不信任，并没有中立中央机构的情况下，能够做到互相协作。



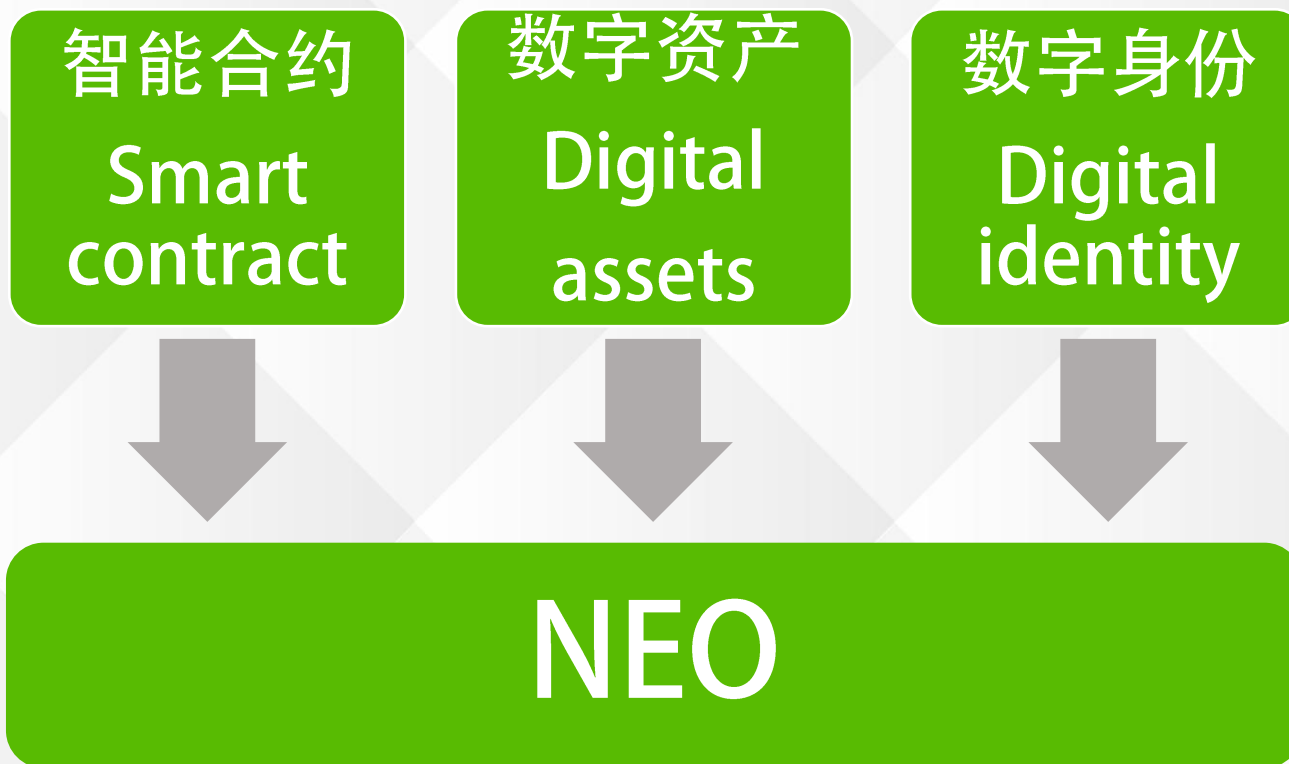
■ NEO: 智能新经济

Digital Assets For Everyone

Smart Economy



NEO: 智能新经济



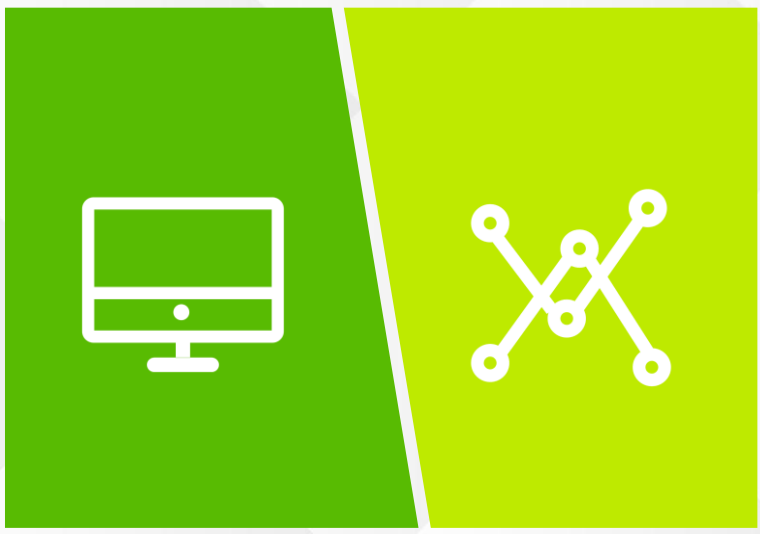
什么是智能合约 What is Smart Contract ?

1994 密码学家尼克萨博 (Nick Szabo) 最先提出智能合约理念

智能合约

“智能合约是指能够自动执行合约条款的计算机程序”

Smart contract :
Auto-execution of
computer programs



区块链

“区块链为智能合约提供的可靠的执行环境”

Blockchain: a sound
environment
for smart contract

■ NEP5 Token Standard

Global Asset

Contract Asset

数字资产

NEP5 Token Standard

```

public class ContractAsset : FunctionCode
{
    public static object Main(string operation, params object[] args)
    {
        switch (operation)
        {
            case "create":
                return Create((string)args[0], (BigInteger)args[1], (byte[])args[2]);
            case "transfer":
                return Transfer((byte[])args[0], (byte[])args[1], (BigInteger)args[2]);
            default:
                return false;
        }
    }

    public static byte[] Create(string name, BigInteger amount, byte[] owner)
    {
        Contract contract = Blockchain.GetContract(ExecutionEngine.ExecutingScriptHash);
        byte[] script = contract.Script.Concat(name.AsByteArray());
        contract = Contract.Create(script, new byte[] { 5, 16 }, 5, true, name, "1.0.0-preview1", owner.AsString(), "", name);
        Storage.Put(contract.StorageContext, owner, amount.ToByteArray());
        return Hash160(contract.Script);
    }

    public static bool Transfer(byte[] from, byte[] to, BigInteger value)
    {
        if (value <= 0) return false;
        if (from.Length != 33 || to.Length != 33) return false;
        if (!Runtime.CheckWitness(from)) return false;
        byte[] data = Storage.Get(Storage.CurrentContext, from);
        if (data == null) return false;
        BigInteger available = new BigInteger(data);
        if (available < value) return false;
        available -= value;
        Storage.Put(Storage.CurrentContext, from, available.ToByteArray());
        data = Storage.Get(Storage.CurrentContext, to);
        if (data == null)
            available = 0;
        else
            available = new BigInteger(data);
        available += value;
        Storage.Put(Storage.CurrentContext, to, available.ToByteArray());
        return true;
    }
}

```



■ NEP5 Token Standard

钱包

交易所

智能合约

标准



■ NEP5 Token Standard

Neo Enhancement Proposal

■ NEP5 Token Standard

BIP: Bitcoin Improvement Proposal

EIP: Ethereum Improvement Proposal



NEP5 Token Standard

Table of Contents

#	Title	Author	Type	Status
1	NEP Purpose and Guidelines	Erik Zhang	Meta	Active
2	Passphrase-protected private key	Erik Zhang	Standard	Accepted
3	Wallet Standard		Standard	Stub
4	URI Scheme		Standard	Stub
5	Token Standard	llwlvllll, luodanwg, tanyuan, Alan Fong	Standard	Accepted
	Superconductive Exchange		Standard	Stub
	Dynamic Sharding		Standard	Stub
	Compact Block Relay		Standard	Stub
	Peer Authentication		Standard	Stub
	Aggregate Signature		Standard	Stub
	SM2 Cryptography		Standard	Stub
	Homomorphic Encryption		Standard	Stub
	Zero-knowledge proof		Standard	Stub
	Stealth Addresses		Standard	Stub
	NeoID		Standard	Stub
	NeoFS		Standard	Stub
	NeoX		Standard	Stub
	NeoQS		Standard	Stub

NEP

■ NEP5 Token Standard

Is NEO token an ERC20 token

■ NEP5 Token Standard

比特币：The King of Tokens

以太坊：Tokens Everywhere



■ NEP5 Token Standard

ERC20: ICO的催化剂

```
1 // https://github.com/ethereum/EIPs/issues/20
2 contract ERC20 {
3     function totalSupply() constant returns (uint totalSupply);
4     function balanceOf(address _owner) constant returns (uint balance);
5     function transfer(address _to, uint _value) returns (bool success);
6     function transferFrom(address _from, address _to, uint _value) returns (bool success);
7     function approve(address _spender, uint _value) returns (bool success);
8     function allowance(address _owner, address _spender) constant returns (uint remaining);
9     event Transfer(address indexed _from, address indexed _to, uint _value);
10    event Approval(address indexed _owner, address indexed _spender, uint _value);
11 }
```

■ NEP5 Token Standard

ERC20

ERC223



NEP5 Token Standard

```
1 public static Object Main(object firstArg, params object[] args)
2 {
3     if (Runtime.Trigger == TriggerType.Verification)
4     {
5         byte[] signature = (byte[])firstArg;
6         return VerifySignature(Owner, signature);
7     }
8     else if (Runtime.Trigger == TriggerType.Application)
9     {
10        string operation = (string)firstArg;
11        if (operation == "deploy") return Deploy();
12        if (operation == "mintTokens") return MintTokens();
13        if (operation == "totalSupply") return TotalSupply();
14        if (operation == "name") return Name();
15        if (operation == "symbol") return Symbol();
16        if (operation == "transfer")
17        {
18            if (args.Length != 3) return false;
19            byte[] from = (byte[])args[0];
20            byte[] to = (byte[])args[1];
21            BigInteger value = (BigInteger)args[2];
22            return Transfer(from, to, value);
23        }
24        if (operation == "balanceOf")
25        {
26            if (args.Length != 1) return 0;
27            byte[] account = (byte[])args[0];
28            return BalanceOf(account);
29        }
30        if (operation == "decimals") return Decimals();
31    }
32    return false;
33 }
```

NEP5 Protocol

NEO The Smart Contract

Market Place

The image shows a screenshot of the Visual Studio code editor with a smart contract code file open. The code is written in C# and includes the following lines:

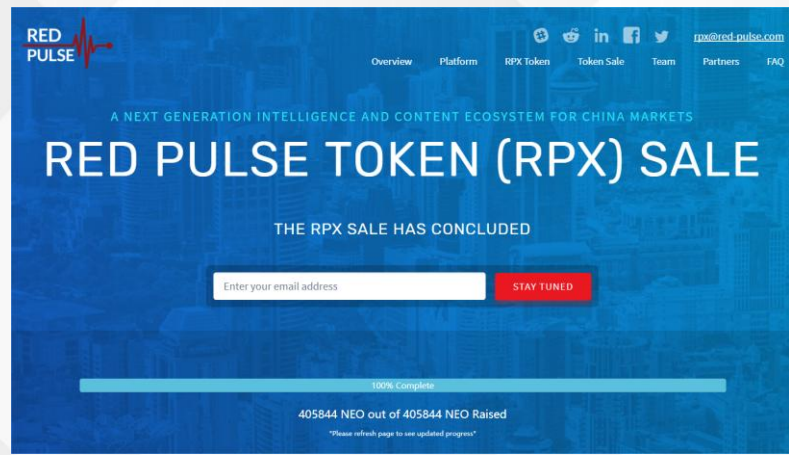
```
1 using AntShares.SmartContract.Framework;  
2 using AntShares.SmartContract.Framework.Services.AntShares;  
3 using System;  
4 using System.Numerics;  
5  
6 namespace SmartContract1  
7 {  
8     public class Contract1 : FunctionCode  
9     {  
10        public static void Main()  
11        {  
12            Storage.Put(Storage.CurrentContext, "Hello", "World");  
13        }  
14    }  
15 }  
16
```

Overlaid on the screenshot are several logos representing different programming languages and environments:

- Microsoft .NET**: A large blue logo with the text "Microsoft .NET" overlaid on the code.
- Java**: A red logo with the text "Java" overlaid on the code.
- Kotlin**: A logo with the text "Kotlin" overlaid on the right side of the code editor.
- Go**: A logo featuring a blue gopher character in a glass jar with the text "Go" below it, overlaid on the bottom left of the code editor.
- JavaScript**: A large yellow logo with the text "JS" overlaid on the bottom center of the code editor.
- Python**: A logo with the text "python" overlaid on the bottom right of the code editor.

.NET CORE The Application

实践-[RPX](#)



.NET CORE The Application

实践-[1445025](#)区块

RPX ICO

北京时间 2017.10.08

Round1 21:00

Round2 22:00
















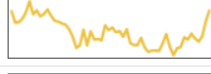




Block [1fa6e8f5fd427ac0c1bb5acc078686cc9a6413492f7a14c141834f99a4c939e7](#)

- Date 2017-10-08 Time 14:01:44
- Height 1445025
- Transactions count 3242
- Merkle Tree Root 9053c0bd86d2566f4359b1e6196a039fb6ded0832216e03b2bb5af3b9071c049
- Next Block Hash [576190c5d6a84253337eb0a007b89642ae31ce61d033d1480220da6f8420d129](#)
- Previous Block Hash [173e2026426671ab122b73570dc731a8fad937f9e3d6eec20e9b95805fadad10](#)
- Data Size 1138099 bytes



NEO: 智能新经济

市值排名

All ▾		Coins ▾	Tokens ▾	USD ▾	Next 100 →		View All
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$94,087,657,146	\$5658.00	\$1,836,880,000	16,629,137 BTC	-0.91%	
2	 Ethereum	\$30,429,165,546	\$319.79	\$471,389,000	95,153,587 ETH	-5.56%	
3	 Ripple	\$9,426,548,340	\$0.244645	\$553,910,000	38,531,538,922 XRP *	-11.96%	
4	 Bitcoin Cash	\$6,070,818,125	\$363.47	\$846,524,000	16,702,575 BCH	15.76%	
5	 Litecoin	\$3,237,951,307	\$60.62	\$200,202,000	53,416,907 LTC	-5.36%	
6	 Dash	\$2,294,388,092	\$300.83	\$44,060,400	7,626,910 DASH	-1.54%	
7	 NEM	\$1,958,976,000	\$0.217664	\$5,430,770	8,999,999,999 XEM *	-1.31%	
8	 NEO	\$1,603,150,000	\$32.06	\$56,709,100	50,000,000 NEO *	14.69%	
9	 Monero	\$1,440,161,808	\$94.56	\$39,978,200	15,230,589 XMR	0.00%	
10	 BitConnect	\$1,391,140,158	\$193.40	\$13,669,700	7,193,109 BCC	-1.27%	

■ NEO FUTURE

NEO * NEP5 = Smart Economy



THANKS!

for watching

林鹏涛

Peter Lin