Neo White Paper

A distributed network for the Smart Economy

Neo design goals: Smart Economy

Neo is the use of blockchain technology and digital identity to digitize assets, the use of smart contracts for digital assets to be self-managed, to achieve "smart economy" with a distributed network.

Digital Assets

Digital assets are programmable assets that exist in the form of electronic data. With blockchain technology, the digitization of assets can be decentralized, trustful, traceable, highly transparent, and free of intermediaries. On the Neo blockchain, users are able to register, trade, and circulate multiple types of assets. Proving the connection between digital and physical assets is possible through digital identity. Assets registered through a validated digital identity are protected by law.

Neo has two forms of digital assets: global assets and contract assets. Global assets can be recorded in the system space and can be identified by all smart contracts and clients. Contract assets are recorded in the private storage area of the smart contract and require a compatible client to recognize them. Contract assets can adhere to certain standards in order to achieve compatibility with most clients.

Digital Identity

Digital identity refers to the identity information of individuals, organizations, and other entities that exist in electronic form. The more mature digital identity system is based on the PKI (Public Key Infrastructure) X.509 standard. In Neo, we will implement a set of X.509 compatible digital identity standards. This set of digital identity standards, in addition to compatible X.509 level certificate issuance model, will also support Web Of Trust point-to-point certificate issuance model. Our verification of identity when issuing or using digital identities includes the use of facial features, fingerprint, voice, SMS and other multi-factor authentication methods. At the same time, we will also use the blockchain to replace the Online Certificate Status Protocol (OCSP) to manage and record the X.509 Certificate Revocation List (CRL).

Smart Contract

The smart contract was first proposed by the cryptographer Nick Szabo in 1994, only five years after the creation of the World Wide Web. According to Szabo's definition: When a pre-programmed condition is triggered, the smart contract will execute the corresponding contract terms. Blockchain technology provides us with a decentralized, tamper-resistant, highly reliable system in which smart contracts are very useful. Neo has an independent smart contract system: NeoContract.

The NeoContract smart contract system is the biggest feature of the seamless integration of the existing developer ecosystem. Developers do not need to learn a new programming language but use C#, Java and other mainstream programming languages in their familiar IDE environments (Visual Studio, Eclipse, etc.) for smart contract development, debugging and compilation. Neo's Universal Lightweight Virtual Machine, NeoVM, has the advantages of high certainty, high concurrency, and high scalability. The NeoContract smart contract system will allow millions of developers around the world to quickly carry out the development of smart contracts. NeoContract will have a separate white paper describing the implementation details.

Application and Ecosystem

Ecosystem is the vitality of the open source community. In order to achieve the goal of an intelligent economic network, Neo will be committed to the development of its ecosystem, providing mature development tools, improving development of documents, organizing education and training activities, and providing financial support. We plan to support the following Neo-based applications and ecology and to reward improvements to the design of the experience:

Node Program

- A fully functioning Full node PC program
- A light node PC program with a better user experience
- Web / Android / iOS clients that do not need to synchronize with the blockchain
- Hardware wallet

Blockchain Explorer

SDK Development Kit

- Support Java / Kotlin, .NET C # / VB, JavaScript / Typescript, Python, Go

Smart Contract Compiler and IDE Plugin

- C# / VB.Net / F#, Visual Studio
- Java / Kotlin, Eclipse
- C / C++ / GO
- JavaScript / TypeScript
- Python / Ruby

Decentralized Applications

- Smart fund
- AI-assisted legal smart contract
- Social networking
- Automated tokens liquidity providers
- Decentralized exchange
- Secure communication protocol
- Data exchange market
- Intellectual property trading market
- Prediction market
- Advertising market
- Hashpower market
- GAS market

Neo Management Model

Economic Model

Neo has two native tokens, NEO (abbreviated symbol NEO) and GAS (abbreviated symbol GAS).

NEO, with a total of 100 million tokens, represents the right to manage the network. Management rights include voting for bookkeeping, Neo network parameter changes, and so on. The minimum unit of NEO is 1 and tokens cannot be subdivided.

GAS is the fuel token for the realization of Neo network resource control, with a maximum total limit of 100 million. The Neo network charges for the operation and storage of tokens and smart contracts, thereby creating economic incentives for consensus nodes and preventing the abuse of resources. The minimum unit of GAS is 0.00000001.

In the genesis block of the Neo network, 100 million NEOs are generated, GAS has not yet been generated. 100 million GAS, corresponding to the 100 million NEO, will be generated through a decay algorithm in about 22 years time to address holding NEO. If NEO is transferred to a new address, the subsequent GAS generated will be credited to the new address.

The Neo network will set a threshold by voting to exempt GAS from a certain amount of transfer transactions and smart contract operations to enhance the user experience. When a large amount of spam transactions occur, NeoID can be used to prioritize transactions and smart contracts with qualified identities. Transactions and smart contracts with no qualifying digital identities can get priority by paying GAS.

Distribution Mechanism

NEO distribution:

NEO's 100 million tokens is divided into two portions. The first portion is 50 million tokens distributed proportionally to supporters of NEO during the crowdfunding. This portion has been distributed.

The second portion is 50 million NEO managed by the Neo Council to support Neo's long-term development, operation and maintenance and ecosystem. The NEO in this portion has a lockout period of 1 year and is unlocked only after October 16, 2017. This portion will not enter the exchanges and is only for long-term support of Neo projects. The plans for it are as below:

- 10 million tokens (10% total) will be used to motivate Neo developers and members of the Neo Council
- 10 million tokens (10% total) will be used to motivate developers in the Neo ecosystem
- 15 million tokens (15% total) will be used to cross-invest in other block-chain projects, which are owned by the Neo Council and are used only for Neo projects
- 15 million (15% total) will be retained as contingency
- The annual use of NEO in principle shall not exceed 15 million tokens

GAS distribution:

GAS is generated with each new block. The initial total amount of GAS is zero. With the increasing rate of new block generation, the total limit of 100 million GAS will be achieved in about 22 years. The interval between each block is about 15-20 seconds, and 2 million blocks are generated in about one year.

Each year around 2 million blocks will be generated and the initial generation will be 8 GAS per block. There will be an annual reduction of 1 GAS per block, per year, to coincide with the passing of every 2 million blocks. The reduction will continue down to just 1 GAS per block and will be held at that rate for around 22 years. After the 44 millionth block the total GAS generated will have reached 100 million and from this point there will be no further generation of GAS from new blocks.

According to this release curve, 16% of the GAS will be created in the first year, 52% of the GAS will be created in the first four years, and 80% of the GAS will be created in the first 12 years. These GAS will be distributed proportionally in accordance with the NEO holding ratio, recorded in the corresponding addresses. NEO holders can initiate a claim transaction at any time and claim these GAS tokens at their holding addresses.

Governance mechanism

Chain governance: NEO token holders are the network owners and managers, managing the network through voting in the network, using the GAS generated from NEO to utilize the functions in the network. NEO tokens can be transferred.

Off-chain governance: Neo Council consists of the founding members of the Neo project, under which the management committee, technical committee and the secretariat, respectively, are responsible for strategic decision-making, technical decision-making and specific implementation. The Neo Council is responsible to the Neo community for the promotion and development of Neo ecosystem as its primary objective.

Neo technology implementation

Consensus mechanism: dBFT

The dBFT is called the Delegated Byzantine Fault Tolerant, a Byzantine fault-tolerant consensus mechanism that enables large-scale participation in consensus through proxy voting. The holder of the NEO token can, by voting, pick the consensus node it supports. The selected group of consensus nodes, through BFT algorithm, reach a consensus and generate new blocks. Voting in the Neo network continues in real time, rather than in accordance with a fixed term.

The dBFT provides fault tolerance of $f = \lfloor (n-1) / 3 \rfloor$ for a consensus system consisting of n consensus nodes. This fault tolerance also includes both security and availability, resistant to general and Byzantine failures, and is suitable for any network environment. dBFT has good finality, meaning that once confirmations are final, the block can not be bifurcated, and the transaction will not be revoked or rolled back.

In the Neo dBFT consensus mechanism, taking about 15 to 20 seconds to generate a block, the transaction throughput is measured up to about 1,000TPS, which is excellent performance among the public chains. Through appropriate optimization, there is potential to reach 10,000TPS, allowing it to support large-scale commercial applications.

The dBFT combines digital identity technology, meaning the consensus nodes can be a real name of the individual or institution. Thus, it is possible to freeze, revoke, inherit, retrieve, and ownership transfer due to judicial decisons on them. This facilitates the registration of compliant financial assets in the Neo network. The Neo network plans to support such operations when necessary.

Smart contract system: NeoContract

Neo's smart contract system consists of three parts:

NeoVM - Universal Block Chain Virtual Machine:

NeoVM is a lightweight, general-purpose virtual machine whose architecture is very close to the JVM and .NET Runtime, similar to a virtual CPU that reads and executes instructions in the contract in sequence, performs process control based on the functionality of the instruction operations, logic operations and so on. It has a good start-up speed and versatility, is very suitable for small programs such as smart contracts, can also be ported to non-blockchain systems, or integrated with the IDE to provide an optimal development experience. NeoVM's functionality can be extended, like introducing a JIT (real-time compiler) mechanism, thereby enhancing the efficiency of the implementation.

InteropService - Interoperable Services:

Used to load the blockchain ledger, digital assets, digital identity, persistent storage area, NeoFS, and other underlying services. They are like virtual machines that are provided for virtual machines, enabling smart contracts to access these services at run time to achieve some advanced functionality. Through this low-coupling design, **NeoVM can be ported to any blockchain or even non-blockchain system used, increasing the utility of the smart contracts.**

DevPack - Compiler and IDE plugin:

DevPack includes the high-level language compiler and the IDE plug-in. Because NeoVM's architecture is very similar to JVM and .NET Runtime, the compilers in DevPack can compile Java byte code and .NET MSIL into NeoVM's instruction set. Developers using main stream languages like Java / Kotlin/ C# do not need to learn new languages and will be able to immediately start developing smart contracts in VS, Eclipse and other familiar IDE environments. **This greatly reduces the learning curve for developing smart contracts, allowing us to easily build a vibrant community around NeoContract.**

NeoContract can create a smart contract call tree through static analysis before running a smart contract. **Through the deterministic call tree, the Neo node can dynamically fragment the smart contract to achieve theoretically unlimited expansion** , which overcomes the "jamming effect" caused by the static fragmentation of other block chain systems.

Cross-chain interoperability agreement: NeoX

NeoX is a protocol that implements cross-chain interoperability. NeoX is divided into two parts: "cross-chain assets exchange protocol" and "cross-chain distributed transaction protocol."

Cross-chain assets exchange agreement:

NeoX has been extended on existing double-stranded atomic assets exchange protocols to allow multiple participants to exchange assets across different chains and to ensure that all steps in the entire transaction process succeed or fail together. In order to achieve this function, we need to use NeoContract function to create a contract account for each participant. If other blockchains are not compatible with NeoContract, they can be compatible with NeoX as long as they can provide simple smart contract functionality.

Cross-chain distributed transaction protocol:

Cross-chain distributed transactions mean that multiple steps of a transaction are scattered across different blockchains and that the consistency of the entire transaction is ensured. This is an extension of cross-chain assets exchange, extending the behavior of assets exchange into arbitrary behavior. In layman's terms, NeoX makes it possible for cross-chain smart contracts where a smart contract can perform different parts on multiple chains, either succeeding or reverting as a whole. This gives excellent possibilities for cross-chain collaborations and we are exploring cross-chain smart contract application scenarios.

Distributed Storage Protocol: NeoFS

NeoFS is a distributed storage protocol that utilizes Distributed Hash Table (DHT) technology. NeoFS indexes the data through file content (Hash) rather than file path (URI). Large files will be divided into fixed-size data blocks that are distributed and stored in many different nodes.

The main problem with this type of system is the need to find a balance between redundancy and reliability. NeoFS plans to solve this contradiction by means of token incentives and the establishment of backbone nodes. Users can choose the reliability requirements of the file. Files with low reliability requirements can be stored and accessed for free or almost free. Stable and reliable services for files with high reliability requirement will be provided by backbone nodes.

NeoFS will serve as one of the InteropService interoperability services under the NeoContract system, enabling smart contracts to store large files on the blockchain and set access for those files. In addition, NeoFS can be combined with digital identity so that digital certificates used by digital identities can be assigned, sent, and revoked without a central server to manage them. In the future, the old block data can be stored in NeoFS, so that most of the full nodes can release the old data for better scalability and at the same time, ensure the integrity of historical data.

Anti-quantum cryptography mechanism: NeoQS

The emergence of quantum computers poses a major challenge to RSA and ECC-based cryptographic mechanisms. Quantum computers can solve the large number of decomposition problems (which RSA relies on) and the elliptic curve discrete logarithm (which ECC relies on) in a very short time. NeoQS (Quantum Safe) is a lattice-based cryptographic mechanism. At present, quantum computers do not have the ability to quickly solve the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which is considered to be the most reliable algorithm for resisting quantum computers.

Summary

Neo is a distributed network that combines digital assets, digital identities and smart contracts. The Neo system will use DBFT, NeoX, NeoFS, NeoQS and many other original technologies, as the infrastructure for the intelligent economy of the future.