

NEO Super

White Paper

V. 1.0

Table of Contents

Executive summary	2
1. Technical background information	3
1.1. Understanding NEO	3
1.2. NEO – advantages over Ethereum	4
1.3. NEO issues	5
1.4. Understanding forks	6
1.5. Snapshots	8
1.6. Forkability of NEO	8
2. Introducing NEO Super	10
2.1. Connection to NEO	10
2.2. Snapshot and distribution	11
2.3. Mining in the Ethereum network	11
2.4. Multiplatform web client	12
2.5. Digital and digitized assets	13
2.6. Asset marketplace	14
2.7. Second-layer protocol support	15
2.8. Summing up	18

Executive summary

As the first wave of the post-industrial revolution is drawing to a close, we are moving ever nearer towards a true smart economy. This economy will be characterized by an increased independence of individuals from centralized authorities, higher speed of transactions, disintermediation, lower costs, and improved cross-border communication. The perennial issue of trust in business dealings will be resolved thanks to the use blockchain technology and smart contracts, which permit zero-cost, instant cross-border payments and simplify verification of contract compliance.

At the same time, the blockchain technology itself is undergoing a profound transformation. Its ability to scale will soon be greatly enhanced by the emergence of second-layer protocols, and running decentralized applications will become much more affordable. Cryptocurrencies and dApps will stop being an exotic novelty for the most tech-savvy and become an everyday reality.

NEO Super intends to become an integral part of this transformation, helping to facilitate the move to the smart economy. The project proposes a convenient environment for launching new digital assets and digitizing real-life assets in accordance with the principles behind existing NEO blockchain. On the other hand, NEO Super introduces numerous advantages of the Ethereum network, such as scaling protocols, mining opportunities, and an easy-to-use API for launching new dApps.

The present document outlines the technical background necessary for understanding the objectives of NEO Super, including forks, scaling protocols, and different mining algorithms. Further, the White Paper examines specific technical features of NEO Super and its benefits for the holders of NEO coins. The grounds for using a snapshot of the NEO network as basis for distribution NEO Super (NEOX) coins – as opposed to holding an ICO – are also explained.

NEO Super both implements a number of concepts inherent to NEO (digitization of assets, digital identities, etc.) and introduces a range of benefits for token holders, miners, and digital entrepreneurs. This makes the new proposed cryptocurrency a successful combination of the advantages of the two systems: NEO and Ethereum. At the same time, NEO Super eliminates a number of weaknesses present in these networks, such as the excessive centralization of NEO and slow speeds common to Ethereum.

1. Technical background information

NEO Super is an ERC20-compatible project that merges some of the most successful principles on which NEO is based with advantages provided by the Ethereum network: from mining opportunities to Lightning Network support. In order to understand what NEO Super proposes to do and why it will benefit the cryptocurrency community at large, it is important to have a clear idea of some blockchain basics. In this section, we provide a detailed analysis of the strengths of NEO, its potential weaknesses, and its differences from Ethereum. We also explain the difference between different types of cryptocurrency forks and examine the possibility of forks on the NEO network. The basics of the Byzantine Fault Tolerance mechanism are explained, as well as the algorithms of Proof-of-Work vs Proof-of-Stake and importance of snapshots for the process of forking.

1.1. Understanding NEO

NEO is the first large cryptocurrency project in China, with a total market capitalization of over 1 billion dollars as of October 2018. It has the advantage of being backed by the government of China and a number of leading Chinese businesses, including Alibaba. Like Ethereum, NEO is designed as a platform that can hold ICOs, dApps (decentralized applications), and smart contracts. The system's main proclaimed objective is to simplify the transition to a "smart economy" based on digitization of real-life assets. Ownership of such assets is verified by means of a digital identity (which can belong to an individual, organization, company, etc.). To authenticate a digital identity, the NEO network uses a complex procedure that includes facial recognition, fingerprints, sms messages, emails, etc.

NEO uses two types of crypto assets in the network. The first – NEO coins themselves – act as shares, that is, they give their holder ownership of a part of the network. The total supply of NEO is limited to 100 million, and the circulating supply equals 65 000 000. All NEO coins were premined during the creation of the genesis block at the moment of launch. NEO is not divisible – therefore, the smallest amount of NEO anyone can hold is 1.

The second asset, somewhat confusingly known as GAS, is being generated according to a special algorithm and will reach its maximum supply in about 22 years. GAS is used to power transactions on the NEO network, such as deployment of smart contracts. GAS is provided to NEO holders as dividends. So for instance, a holder of 100 NEO will receive a GAS reward of about 10 GAS per year (circa \$50 with the current GAS price), resulting in a ROI of about 3%.

On the other hand, GAS works just like gas on the Ethereum network, paying for various operations on the blockchain. Since the amount of GAS rewards generated may not be enough to pay for all the transactions required by a user, additional purchases of GAS may be required.

1.2. NEO – advantages over Ethereum

Even though NEO allows to create and deploy smart contracts and ICOs, just like Ethereum, it has a number of attractive advantages over the Ethereum network:

1) Smart contracts can be written using C# and Java (Python is to be added in the near future), meaning that developers do not need to learn a new programming language in order to write smart contracts for the NEO blockchain. By contrast, developing a smart contract on Ethereum requires the knowledge of Solidity.

2) Improved consensus protocol – NEO uses a proof-of-stake consensus protocol, while Ethereum uses proof-of-work (though a hybrid PoS/PoW protocol is being tested). This means that in NEO the node to verify a transaction is chosen selected by how many NEO coins they hold in the form of a locked deposit (stake) and partly by how long they have held them. This algorithm requires much less computing power, allowing average users to participate without purchasing mining equipment. It is also more sustainable and cheap, as well as much more environmentally-friendly. Since neither NEO coins nor GAS can be mined, nodes that complete blocks on the network should be called forgers rather than miners, and what they receive are transaction fees, not block rewards. On the other hand, Ethereum is still fully proof-of-work: miners compete to solve mathematical puzzles to decide who gets to complete a block and get a reward. Proof-of-work requires much more computing power and electric energy to run, making it expensive and environmentally unsustainable.

3) Delegated Byzantine Fault Tolerance protocol – this consensus algorithm allows the keep the system live and running smoothly even when some of its nodes (up to 1/3) experience failure or act maliciously – that is, intentionally transmit incorrect information. Byzantine fault tolerance mechanism allows to reduce energy consumption, since the system does not require a round of confirmations from all the miners before finalizing a block. Ethereum has implemented the protocol in a hard fork in October 2017, but NEO has featured it from the start.

4) Network capacity – the NEO network can in theory handle thousands of transactions per second, while the Ethereum network's current capacity is only about 25 transactions per second, which often results in delays processing payments.

5) Chinese government support – many believe that the potential of NEO is larger than that of Ethereum due to its inherent compliance with the state regulations in China. What's more, the founder of NEO Da Hongfei was asked to advise the Chinese authorities on the best course of action regarding cryptocurrency exchanges and ICOs – and he famously recommended temporarily banning them in order to reduce the number of scams and failures and better utilize the potential of blockchain. In the world where official regulation of cryptocurrencies is becoming ever stronger, the support of China can prove crucial to the future of NEO.

6) Protection against quantum computers. Even though no commercial quantum computer is available on the market yet, they will appear in the next couple of years; many believe that quantum computers will represent a deadly threat to cryptocurrencies, being able to hack into blockchain networks and private keys. Ethereum has no valid protection against quantum computers so far, while the developers of NEO have apparently already developed a mechanism called NeoQS.

1.3. NEO issues

With all the advantages that NEO has over Ethereum, it also suffers from a number of issues that prevent the network from achieving its full growth potential.

1) System speed – in spite of the advertised capacity of thousands of transactions per second, the actual speeds on the network are usually much slower, and in periods when an ICO is running, one block can take minutes to complete. On some occasions, the network experienced outages lasting up to two hours.

2) No mining – since all NEO coins were pre-mined during the creation of the very first block, no new NEO can be created. GAS cannot be mined, either, since it is automatically generated by the system. Thus, the network cannot profit from the attention of the mining community. Pre-mining all the coins concentrates vast amounts of a new cryptocurrency in the hands of the developers and early supporters, creating a level of centralization that – as many believe – goes against the very ideology of cryptocurrencies.

3) Centralization and regulation – while the support of the Chinese government can be good for the future of NEO in China, it requires a high level of control of both the team and the regulator over the network. The rules of the game can be changed at any moment to comply with new laws and rules.

4) High fees – among all leading blockchain platforms that allow for deployment of new cryptoassets (Ethereum, EOS, etc.), NEO is currently the most expensive. Launching an asset will cost between 100 and 1000 GAS, depending on the type and complexity, which with the current (as of October 2018) GAS price of \$5.78 means an investment between \$578 and \$5780. Launching an ICO carries a fixed fee of 5000 GAS - \$28900! This is prohibitively expensive for most ICO teams. For comparison: deploying even a complex ICO smart contract on Ethereum generally doesn't cost more than \$100.

5) Smart contract vulnerabilities. To date, two important vulnerabilities have been discovered in the way NEO handles smart contracts. The first is the so-called storage injection vulnerability (NEP-5) – the potential possibility to increase a token's total supply by sending more tokens to the contract's Total Supply string used as an address. While new tokens cannot be created this way, the contract's owner's address can in theory be changed, and consequences for advanced dApps can be disastrous.

The second vulnerability recently discovered (August 2018) is the DoS attack vulnerability, which can allow a hacker to recreate a classic DoS (denial of service) attack. In this case, a malicious smart contract can cause all network nodes to crash as it propagates across the NEO blockchain. Of course, launching such a smart contract would require the hacker to pay the required high fee. The vulnerability was patched a few hours after discovery, but there may be others. NEO is a very promising but still very new platform, so the extent of its security issues remains unclear.

1.4. Understanding forks

The term “fork” can take various meanings in the cryptocurrency realm, resulting in a lot of confusion. In its simplest form, a fork is a situation when two blocks are creating pointing to the same previous block. In most cases, this is accidental (and happens often in Ethereum and other networks) and is quickly resolved: whichever of the two split chains gets a new block faster becomes the truthful chain, while the transactions in the other are reversed, after which it is abandoned. Such forks are unplanned and usually mean only a delay, not a change to the system.

By contrast, forks that permanently split a chain are more serious and can be both planned or unplanned. Since most cryptocurrencies are open-source, any developer can write and present to the community a potential improvement or enhancement of the existing code. Users who accept a proposed change need to upgrade their software.

In a soft fork, those users who do not perform the required upgrade can still use the network, view new transactions and participate in consensus, but they will lose part of the functionality – for example, they will not be able to complete new blocks and get rewards. In a hard fork, users are not able to use the network without upgrading their software (though they are still able to use the old, unforked version of the network). This is similar to the release of a new version of Windows: users can choose to continue using Windows 7 or 8.1, for example, but newer versions of many applications (such as Photoshop, Office, etc.) will not work on their machine until they upgrade to the latest Windows version.

In some cases, the original developer team includes a hard fork in their project roadmap and presents the necessary upgrade with all the necessary explanations. In such cases, all network users readily accept the fork. Sometimes the need for a hard fork arises suddenly as a result of a hacker attack or a dangerous vulnerability being discovered. Finally, the growth and scaling of a network can require a fork – just like it happened with Ethereum, which introduced its new version (Constantinople) in October 2017. It includes the dBFT (delegated Byzantine Fault Tolerance) protocol, which will allow the network to process many more transactions per second.

Sometimes part of the community doesn't accept the fork (for ideological reasons, for example) and remains behind. In this scenario, the majority that chooses to go ahead with the fork retains the original name of the coin, while the minority that rejects the upgrade essentially keeps using the old coin, but under a new name. The most famous example is probably Ethereum, which split to correct a vulnerability that had led to the collapse of the DAO project (Decentralized Autonomous Organization) after an attack. Those users who could not accept the centralization of control required by the fork still use the “old” Ethereum, but under the name of Ethereum Classic (ETC). Their ideological choice has cost them quite a lot: the price of ETH just before the fork was circa \$13 but has since grown manifold (circa \$200 at the time of writing, but its all-time high was over \$1400 in January 2018). ETC's price, on the other hand, hovers around \$10.

In other cases, hard forks are proposed by users themselves, when the consensus on the network splits. Some developers in the community may find that a serious change is necessary to reduce network fees or increase processing speed. This is exactly what happened with Bitcoin Cash, Litecoin, and Dogecoin, which are all modifications of Bitcoin. In such situations, the community is permanently split, and a new coin is created. To attract users and miners to the new coin, it is usually distributed for free to holders of the old coin in the form of an airdrop. For example, in the recent Bitcoin forks, each BTC holder could receive 1 BCH (Bitcoin Cash), 1 BTG (Bitcoin Gold), 10 BCD (Bitcoin Diamond), and 0.5 BTX (Bitcoin Core). It is important to

note that new coins are awarded for free, so that holders of the old coin do not need to give it up – the very fact of holding BTC, for example, gives the owner the right to claim and collect free new coin. This ensures a wider adoption and circulation on the new coin on the market.

1.5. Snapshots

Shortly before a fork happens, a so-called snapshot of the network is taken – essentially, it is a copy of the whole blockchain that lets fork developers know how many of the old coins each user holds. A snapshot is crucial, since free new coins are distributed in accordance with its data. Sometimes an exact date and time is announced for a snapshot and sometimes the block height (that is, the block number which will be used for the snapshot). A combination of the two methods is possible, when the date is provided long before the fork and an exact blockheight is given shortly before the snapshot. This is useful when the computing power in the network and the resulting hash rate can change very quickly (for instance, with the entrance of a new mining rig), as it happens often with Bitcoin or Ethereum.

It is important to point out that the number of free coins that each holder receives depends on the number of old coins he or she holds at the moment of the snapshot, not at the moment of the fork itself (which can happen hours later, once the first block of the new chain is completed). After the snapshot, users are free to do what they like with their old coins, including selling them. This makes forks an attractive investment instrument, since one may choose to buy some of the “old” coins in order to get new cryptocurrency for free, then sell the old coins and wait for the new currency to get listed at an exchange to sell it, too.

1.6. Forkability of NEO

A lot of misunderstanding and incorrect representations surround the question of NEO forks. To put it simply, NEO cannot be forked in the same way as Bitcoin or Ethereum – that is, there is no way to split the chain and create a new coin based on NEO. The reason for this is the implementation of the delegated Byzantine Fault Tolerance protocol, which requires at least 50% for a consensus on any change. This means that a change to the network can only be accepted or rejected by the network as a whole. If it is accepted, the old chain will be abandoned and the new chain will automatically become the “true” one, to be used by everybody. It is impossible for some of the users to remain with the “old” NEO.

That said, it is possible for the whole NEO network to be upgraded upon the initiative of the developer team and subject to a general vote. As recently pointed out by the founder and CEO

Da Hongfei¹, NEO might need a major upgrade in the future, but it will take at least a year. Such an upgrade would create NEO 3.0 – a more efficient and secure network. It will require such a serious change to the code that a new genesis block may need to be created. In this case, users will not need to do anything – their NEO and GAS coins will be exchanged automatically, and the transfer for developers should be seamless. Old transactions will remain on the NEO 2.0 chain but will be readily available for review.

One instance that has generated significant confusion around NEO’s ability to fork was an accidental fork that happened in September 2018.² The dBFT (delegated Byzantine Fault Tolerance) that NEO uses is not the same as the original scheme (known as Practical Byzantine Fault Tolerance) proposed in the research paper by Castro and Liskov in 1999.³ The original protocol includes three stages to reaching a consensus: pre-prepare, prepare and commit. In NEO and other networks that use dBFT, the last stage – commit – is omitted to make the process faster and less resource-intensive. However, this can lead (in rare cases) to a situation where nodes create two valid blocks with different hashes but the same block heights, which results in an accidental fork. This is exactly what happened to NEO, stalling the consensus. The situation was eventually resolved and one of the chains was selected as the true one. The fork was unexpected and required a vulnerability patch, but it is crucial to note that it was not a planned or specially prepared hard fork. Once again: a “true” hard fork, in which a new NEO-based coin is created, is impossible on the NEO network.

1

<https://www.chepicap.com/en/news/3831/neo-s-da-hongfei-probably-need-a-hard-fork-or-new-genesis-block-for-neo-3-0-.html>

² https://www.reddit.com/r/NEO/comments/97qm27/how_did_neo_fork/

³ <http://pmg.csail.mit.edu/papers/osdi99.pdf>

2. Introducing NEO Super

NEO Super leverages the strong methodological foundation behind NEO (smart economy, crypto assets, digital identity verification) with important practical benefits of Ethereum (mining, Lightning Network, low fees, etc.). In this section, we examine the key features and tools of the NEO Super project, including its mineable ERC20 token, the scheme of early distribution to NEO holders, and various types of digital and digitized assets that can be created using NEO Super. Considerable attention is paid to the issues of user identity verification and second-layer scaling protocols.

2.1. Connection to NEO

As pointed out in the previous section, true hard forks of the Bitcoin/Bitcoin Cash type are impossible on NEO. Thus, NEO Super should not be thought of as a true NEO fork. Rather, it uses some of the most successful principles on which NEO is based to create a more efficient and secure Ethereum-based blockchain environment, at the same time targeting the NEO community. The moment of launch of NEO Super is called a fork for reasons of simplicity, but what is created is in fact an ERC20 token that takes the best from both worlds.

We have decided to mainly address the NEO holders community for several reasons:

- 1) It is altogether smaller, more tightly-knit and forward-looking than the Ethereum community, which is overloaded by newbie users who cannot contribute quality new assets to the network;
- 2) NEO has issues that have already become very clear to users and developers participating in the network and that NEO Super can effectively address;
- 3) NEO network hasn't yet become a fertile ground for scams and undercooked, low-quality projects – the entrepreneurs interested in launching their projects on NEO exhibit a more serious approach to planning and development;
- 4) The concept of smart economy and digitization of real-life assets together with a sophisticated authentication system appeals to the founding team of NEO Super.

It is necessary to point out that the development team of NEO Super is not affiliated with the original NEO team. The prefix NEO in the name of the project is used in accordance with the tradition of naming new forked coins after original cryptocurrencies they fork from (as in Bitcoin Cash and Bitcoin Gold), even though NEO Super is not a real fork of NEO.

2.2. Snapshot and distribution

The initial distribution of free NEO Super (NEOX) coins will be preceded by taking a snapshot of the NEO blockchain. The snapshot is scheduled for November 10, 2018 (20:00 GMT). The exact block height will be announced later.

All users who result to hold NEO coins at the moment of the snapshot will be able to claim free NEOX coins at a 2:1 ratio. For instance, a user who holds 100 NEO will be entitled to 200 free NEOX. Only NEO coins kept in private NEO wallets (such as Ledger Nano S, NEON, NEO-GUI, etc.) will be eligible for the free NEOX reward. Users who keep their NEO in wallets at exchanges will not be able to claim free coins. A possible exception would be an exchange that adds NEOX support ahead of the snapshot.

After the snapshot is taken, NEO holders will be free to sell or transfer their NEO tokens as they please – they will still be able to claim their reward.

The total NEOX supply is limited to 225 000 000 coins, out of which 20 million are reserved for further improvement and development of the system and 5 million for the bounty campaign.

2.3. Mining in the Ethereum network

For a long time, there were no mineable ERC20 tokens in the Ethereum blockchain – moreover, many users still believe that such tokens cannot be mined. Instead of being created by miners, such tokens are traditionally pre-minted by the smart contract owner and distributed to backers during an ICO or for free in the form of an airdrop. The problem with this scheme is that ICO tokens are considered securities by regulators in more and more countries, since they represent a transfer of value that allows the token holder to sell the token later and earn a profit; the resulting income (that is, an eventual increase in the price of the token) does not result from any effort made by the token holder. Such a token sale model – making a contribution to a common enterprise with the goal of earning profit that stems from other people's efforts – is what constitutes a security according to the famous Howey test (named after a court case presided by the US judge Howey and used by the US Securities Commission, or SEC, to determine if a certain asset is a security).

On the other hand, mined tokens or coins cannot be considered a security from this point of view, since they require a considerable effort on the part of a miner to create (by solving

mathematical puzzles in the Proof-of-Work consensus protocol). For this reason, altcoins that are mined usually do not attract regulators' attention.

Apart from the regulatory issues, ICOs are subject to a number of other problems, including numerous frauds (known as scams) and frequent failure due to the fact that such projects raise funds without a viable product.

Moving away from the ICO model and pre-minted tokens to mined ERC20 tokens represents a good solution to the ongoing ICO crisis. Creating mineable ERC20 tokens is not only possible but completely feasible, as long as the target difficulty level increases with time along with the increase in hash rate. NEO Super will be just such a token. Its additional advantage lies in the fact that it will allow small independent miners (even beginners) to enter the field, since they will not have to compete with large mining farms. The reward will be set to 5 NEO Super per block. The system will provide a wide range of tools for both individual miners and those who seek to form a pool. We believe that the future of the Ethereum network lies in mined tokens and not in dubious ICOs where founders have full control over token supply.

Not only will NEO Super be mineable – new assets created on the NEO Super blockchain can be designed to be mined, too. While the block rewards model constitutes the most convenient basis for the mining process at the moment, the introduction of major Ethereum upgrades (starting with Constantinople) that introduce the Proof-of-Stake consensus mechanism will make PoS an available option in the near future.

2.4. Multiplatform web client

A user-friendly, multifunctional client app is essential to any cryptocurrency project. Unfortunately, most existing solutions – be it wallets, exchanges, or marketplaces – are overloaded with unnecessary features and feature a steep learning curve that scares off many beginners. The team of NEO Super has developed an easy-to-use yet advanced web client that is optimized for different devices, browsers and platforms. It will provide access to the NEO Super wallet (used to store NEO Super and any assets created on the basis of its blockchain), mining client, and asset marketplace.

The client will feature tools for identity verification, community-building, project promotion, etc. NEO Super wallet can also be used for storing ether and other ERC20 tokens, including those that are not created on the NEO Super network. NEOX (NEO Super tokens) will also be supported by many other popular wallets, such as Trezor.

The development of the web client and other features will be financed out of the proceeds from pre-mining and forked coins allocated for the project's reserve fund.

2.5. Digital and digitized assets

NEO Super will be a sophisticated yet user-friendly environment for launching digital assets of all types: tokens of blockchain-enabled platforms, cryptocurrencies, rights of ownership, shares in startup companies, and so on. NEO Super will provide a complete set of tools for creating a new asset and ensuring its adoption across the community. Digital assets that can be developed and traded using NEO Super include fungible and non-fungible ERC tokens to be used in ICOs, blockchain games, investment projects, and so on. However, existing assets (virtual and physical) can also be converted into digital form and used within the NEO Super network.

The concept of digitized assets that underlies the present NEO blockchain will be further developed in NEO Super to leverage the advantages provided by the Ethereum network and new second-layer scaling protocols (see below). Not only on-chain assets can be transferred and traded – any asset, including a physical object, can potentially be digitized. Put simply, digitization of an asset means creation of a digital proof of ownership that can be transferred with or without physically transferring the asset. A similar scheme already works in our everyday life: for example, selling a car requires making a record of the new owner in the car's identification document. Similarly, buying company stock does not mean physically transferring part of the company's production facilities to the new owner: rather, the change of ownership is recorded. To digitize such assets as a car or a gold bar, a special code (usually a QR code) needs to be physically added to the asset – for instance, stamped somewhere on the surface. For some assets, such as real estate, an address would be enough. Data from the code is then recorded on a blockchain. In case of a sale of such a digitized asset (where an on-chain transfer is not possible), the funds would be stored in a multisig escrow wallet provided by NEO Super until the buyer receives the asset (or a proof that the ownership has really been transferred – as in the case of gold bars stored in a safe vault, for example).

Naturally, the more valuable an asset, the more important it is to verify the identity of its owner or buyer. NEO uses a sophisticated authentication system known as digital identity, and this concept will be enhanced in NEO Super. A whole variety of tools can be used to create a digital identity of a user, and the complexity of authentication will depend on the type of asset that a specific user owns or transfers. For example, ownership or sale of digitized gold bars or shares in the ownership of a company worth thousands of dollars requires a more stringent identity check than a simple exchange of cryptocurrency. Among the tools used to create a digital identity are

facial recognition, fingerprints, digital signature, single-use codes sent by email or sms, and so on. Those NEO Super users who make the effort to go through all the checks will have preferential access to the services of the platform.

2.6. Asset marketplace

All digital and digitized assets created by members of the NEO Super ecosystem will be available in the platform's marketplace. A decentralized voting and selection process will be implemented to rate assets and assess their value and prevent the appearance of risky or fraudulent assets in the marketplace.

As we have pointed out before, all kinds of assets (first digital and, in the near future, digitized real-world assets) can be launched on NEO Super and traded in the marketplace. This means the following, among others:

- utility tokens issued for crowdfunding purposes and to give access to new platforms;
- new cryptocurrencies;
- equity shares in a new company;
- collectible in a blockchain game;
- proof of ownership rights, license, or copyright;
- right to access a real-world, physical service (like the right to use a mining facility, for example);
- tokens giving access to digital content, such as video, ebooks, educational courses, interviews, etc.;
- storage capacity;
- databases and collections of big data.

Digital identities of asset creators and holders will be verified with varying degrees of rigour depending on the category of an asset. This will resolve the issue of conducting a KYC; in particular, which presently plagues many blockchain projects. Whenever an asset cannot be sold or transferred to a citizen or resident of a particular country for reasons of legal restrictions, a startup is forced to conduct an identity check for each potential customer, asking users to supply their IDs, selfies taken with these IDs, and sometimes even bank statements. However, since a KYC is a time-consuming process, many teams choose to rely on costly outside service providers. Those who decide to process KYC applications themselves often find that the workload is simply too great: it takes weeks to process all requests, resulting in delays in distribution of tokens and significant annoyance among token buyers.

Another problem is that every project conducts its own KYC: those users who back numerous platform have to perform virtually the same identity check over and over again, sending the same files and waiting for approval, sometimes for many days. By contrast, thanks to the system of digital identities established by NEO Super, every user will be securely identified from the start and able to participate in all the projects on the marketplace without having to pass a new check every time. At the same time, each digital identity can be enhanced with new data (similar to systems of certificates assigned to users in some payment systems). Thus, identities will come in several types, or levels, from beginner (almost anonymous) to fully certified (a user who has submitted an extensive range of documents and passed all the checks). Each project or asset in the marketplace will be accompanied by a required level of digital identity verification, to be selected by the team of that project. Those users who wish to participate but do not have the necessary identity level yet will be able to submit additional documents and obtain the required identity rank.

Only a minimum fee will be charged for launching an asset, which will distinguish NEO Super from the original NEO blockchain, where, as noted earlier, it costs thousands of dollars to hold a token sale. The use of a second-layer protocol – be it via payment channels or child chains – will allow NEO Super to avoid unnecessary miner fees. Thanks to the same second-layer solutions, exchange of assets on the network will be instantaneous. Affordability, security and speed will be the defining qualities of NEO Super.

2.7. Second-layer protocol support

From the very inception of major blockchains like Bitcoin and Ethereum, it was clear that scaling would eventually become an issue. While the Bitcoin network can currently process up to 25 transactions per second (and the Bitcoin Cash around 60), Ethereum can manage only 15. For comparison: Visa can process over 40 000 transactions per second in peak times, and it is this “Visa barrier” that blockchains ultimately aspire to cross.

The reason for current low speeds is the necessity to obtain confirmations to each transaction from all nodes on the network – which is exactly what makes blockchains so safe and tamper-free. As long as the number of users – and, therefore, transactions – on the network is low, delays are not an issue; however, as the number of transactions grows, users are forced to wait for many seconds – sometimes minutes – for their transaction to go through. Fees factor in, too: all miners on the network have to receive their reward, so transaction fees can become uncomfortably high, especially in case of micropayments, where the sums themselves are small.

It is clear that in a true “smart economy” based on trustless, smart contract-driven payments and digitization of assets, users should not have to wait for their transactions to go through – payments must be instant. Until the system is able to scale properly, such everyday uses of cryptocurrency as paying for a cup of coffee or petrol for one’s car are not feasible. (True, many businesses already accept payments in Bitcoins as a marketing move, but in reality they simply use third-party services to convert receive Bitcoins into fiat currency that is deposited in the company’s account – it is not a sign of real adoption.)

NEO Super, as a project based on the concept of smart economy and free creation of new assets, will necessarily require a scaling mechanism. It has long been understood that the best way to scale a major blockchain is to transfer most of the smaller transactions off the main chain, relieving the load on nodes. While blockchain is extremely secure exactly because records of transactions are validated by all the nodes and stored on-chain, most operations clearly do not need to be stored on the main blockchain. Moreover, they do not require the agreement of all the network members, as long as users performing a transaction between themselves agree to it. Thus, there is a need for a protocol that would allow users to transact with each other without waiting for the general network consensus and paying the fees charged by miners.

Such protocols are already being tested and are known under the general name of second-layer protocols, the first of which to be formulated is the Lightning Network, developed for Bitcoin, Litecoin and other altcoins.⁴ Similar solutions are being tested for the Ethereum blockchain, the main among them being Raiden and Plasma. It is crucial to note that each of these titles is not a specific branded product, but rather a concept that is being worked on by many developers around the world simultaneously.

Second-layer protocols developed for Ethereum take two main forms. In the first, used by Raiden, users establish payment channels with each other and place a deposit into a special shared wallet. Two users who wish to transact with each other both have private keys to such a wallet, and the information about the wallet and the amount of funds in it is recorded on the main Ethereum blockchain. Once the channel is established, the two users essentially transfer some of the funds in the wallet to each other, but the maximum amount that can be sent is limited to the size of the deposit. If users decide to conclude their payment process and transact no more, the channel can be closed and the information about the final ownership structure of funds in it is recorded on the main blockchain again.

In this system, one user can establish many payment channels with other users and send payments via those channels, even if the final recipient doesn’t share a direct channel with the

⁴ <http://lightning.network/lightning-network-paper.pdf>

sender. It is enough to enter the address of the recipient, and the system will find the best route. Since transactions do not need to be recorded on the Ethereum blockchain (essentially all payments are processed off-chain), the fees will be minimal or even equal to zero, and processing will be executed instantaneously.

As of the time of writing (October 2018), only one solution was operational on the Ethereum mainnet – Micro Raiden. This protocol allows one user or platform to receive payments for many other users (“many-to-one” setup) and can be useful to companies selling goods or services, but not to multiple users exchanging assets among themselves. The release of another, more universal solution – Raiden Network – is planned for the next few months.

In a different type of second-layer protocols (the main being Plasma), multiple child chains are created, all stemming from the “root chain” - that is, the main Ethereum network. Each child chain is independent from the others and represents the network of a particular dApp. Users can freely transfer resources from the main chain onto a child chain, which has its own smart contract, nodes and consensus algorithm (which can be different from that of the root chain). When entering a child chain, a user has to attach a collateral to guarantee correct behaviour. All payments are made inside the child chain with minimal fees. A user can choose to leave the child chain at any time, withdrawing their assets to the main chain, which is recorded on the Ethereum blockchain. At the moment of exit, other users are encouraged to challenge the user and point out any malicious behaviour – if the user is caught as having done something wrong while on the child chain, they will lose their collateral. Plasma is not operational yet, but the development process is going quickly.

Both Raiden and Plasma can potentially increase the capacity of the Ethereum network to up to 1 million transactions per second, eliminating bottlenecks and dramatically reducing transaction costs. Some express concerns about security (especially if a lot of micropayments start going through the same nodes, called hubs, which will create some centralization), but it can be expected that large and more important transactions will still go through the main Ethereum blockchain, with smaller dApps using second-layer protocol solutions.

In the context of NEO Super, this means that users who create and trade their own tokenized assets will be able to sell them instantly and without incurring any transaction fees (or almost). Be it tokens of a new project, digitized real-life assets, a share in a digital business – any asset can be securely transferred using a solution similar to Lightning Network. All such solutions work via an API, so that no particular technical skills will be required of NEO Super users. Without such a tool, a viable system of asset exchange is simply impossible.

It is necessary to underline once again that none of the major second-layer solutions and upgrades have been released on the Ethereum mainnet yet, but they will be in the very near future. A drawback of Raiden is the limit that it sets on the total amount of funds that can be transmitted within one payment channel (it cannot exceed the deposit in the shared wallet); however, the fees can be reduced down to zero. With Plasma, all transactions still operate on-chain and involve nodes that are rewarded with a small fee, but security is generally higher. Thus, the NEO Super team has not yet committed to implementing Raiden or Plasma; the choice will be made once at least one of these protocols goes live and can be tested.

2.8. Summing up

NEO Super aims to help build a true smart economy based on trustless, instant, zero-fee transaction. To achieve this aim, the project will implement a hybrid model that leverages the concept the NEO blockchain with the stability of the Ethereum network with an addition of mining functionality. With its asset marketplace, support for second-layer scaling protocols and digital identities, NEO Super is a good solution for many issues that are currently preventing a wider adoption of cryptocurrencies, such as scaling, entry barriers for beginner miners and users, high fees and transaction delays.

The initial distribution of NEO Super will be carried out among current NEO holders after a snapshot taken on November 10, 2018, at which point every user holding NEO will be able to claim free NEO Super (NEOX) coins. Immediately after that, everyone will be welcome to start mining NEOX and developing their own digital assets based on NEO Super. In the upcoming months, NEOX will be listed on several leading exchanges (negotiations are ongoing), and support for scaling protocols such as Plasma or Raiden will be added.

A combination of verified digital assets, user identity authentication tools, user-friendly environment for launching new assets will make NEO Super a true gateway into the smart economy of the future – transparent, trustless, and free from centralized authorities.