**What is Neo Blockchain? Beginners Guide**

An in-depth guide by BlockGeeks

[Back](https://blockgeeks.com/guides/neo-blockchain/)

**1**

[**0**](https://blockgeeks.com/guides/neo-blockchain/#respond)

* [Blockchain 101](https://blockgeeks.com/category/blockchain-101/)

* [Blockchain for business](https://blockgeeks.com/category/blockchain-for-business/)

[Tweet](https://twitter.com/share?original_referer=/&text=What+is+Neo+Blockchain%3F+Beginners+Guide&url=https://blockgeeks.com/guides/neo-blockchain/%3Futm_source%3Dtwitter%26utm_medium%3Dsocial%26utm_campaign%3DSocialWarfare%2FBG&via=Blockgks)

[Share**69**](https://www.facebook.com/share.php?u=https%3A%2F%2Fblockgeeks.com%2Fguides%2Fneo-blockchain%2F%3Futm_source%3Dfacebook%26utm_medium%3Dsocial%26utm_campaign%3DSocialWarfare%2FBG)

[Share**9**](https://www.linkedin.com/cws/share?url=https%3A%2F%2Fblockgeeks.com%2Fguides%2Fneo-blockchain%2F%3Futm_source%3DlinkedIn%26utm_medium%3Dsocial%26utm_campaign%3DSocialWarfare%2FBG)

[Reddit**283**](https://www.reddit.com/submit?url=https://blockgeeks.com/guides/neo-blockchain/&title=What+is+Neo+Blockchain%3F+Beginners+Guide)

**SHARES361**

**Join over 115,115 Members**

**Angel Investors, Startups & Blockchain developers...**

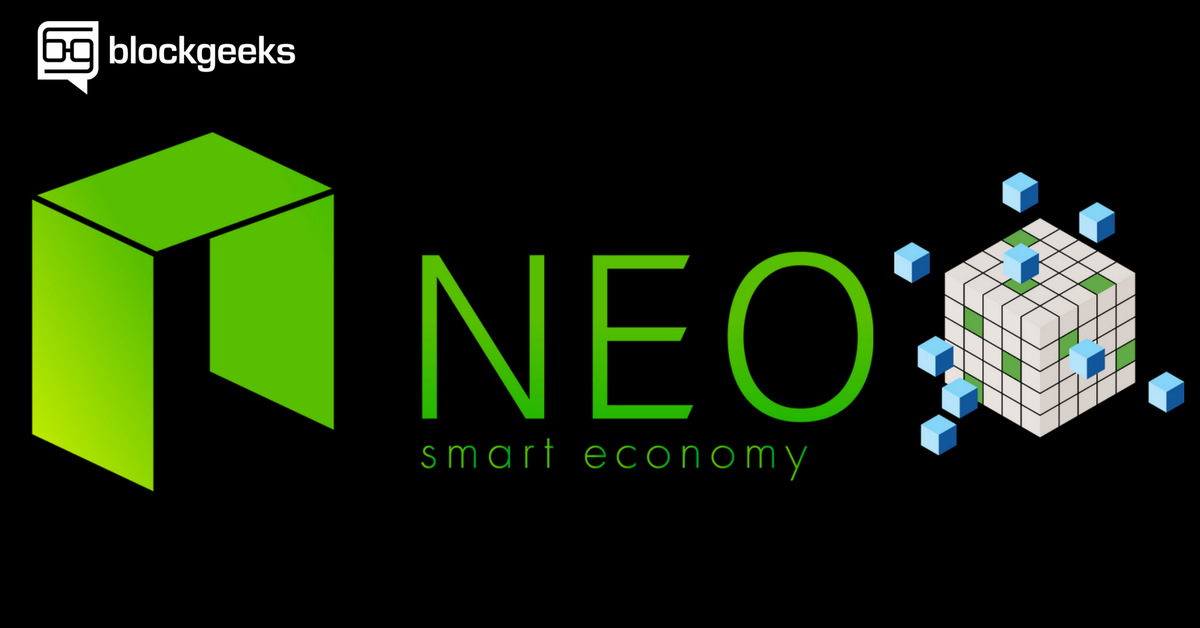
Top of Form

**Yes, Get Access!**

Bottom of Form

No Thanks!

What is Neo Blockchain? Beginners Guide. If you are interested in[cryptocurrency](https://blockgeeks.com/guides/what-is-cryptocurrency/), then there is no way you have not heard of “Neo Blockchain”. Neo, formerly known as Antshares, is often known as the “[Ethereum](https://blockgeeks.com/guides/ethereum/)of China”. While similar to Ethereum, it has some interesting features which deserve a close examination. In this guide we are going to do a deep dive on NEO.

[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/What-is-Neo-Blockchain_-Beginners-Guide.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide)

**The History of Neo Blockchain**

According to [their website](https://neo.org/), Neo is a “non-profit community-based blockchain project that utilizes blockchain technology and digital identity to digitize assets, to automate the management of digital assets using smart contracts, and to realize a “smart economy” with a distributed network.”

Neo’s main aim is to be the distributed network for “smart economy”.  As their website states:

**Digital Assets + Digital Identity + Smart Contract = Smart Economy.**

Neo was developed by Shanghai-based blockchain R&D company “OnChain”. Onchain was founded by CEO Da Hongfei and CTO Erik Zhang. Research on Neo started around 2014. In 2016, Onchain was listed in the Top 50 Fintech Company in China by KPMG.

The Neo Project was funded by two crowdsales. The first crowdsale took place on October 2015 lasting for 10 days during which 17.5 million NEO tokens were sold for $550,000. In the second crowdsale, the remaining 22.5 million NEO tokens were sold for $4.5 million.

**Neo Blockchain and Smart Economy**

As the [Neo website states](https://neo.org/), the three components that makeup Smart Economy are:

* Digital Assets.
* Digital Identity.
* Smart Contract.

**Neo Blockchain and Digital Assets**

A digital asset is anything that exists in binary format and with the right to use. It is critical for a digital entity to have that “right to use” for it to qualify as a digital asset. While it is possible to have digital assets in a centralized environment, it can be extremely risky.

With the advent of the [blockchain](https://blockgeeks.com/guides/what-is-blockchain-technology/), it has become far safer to own digital assets. The blockchain technology makes the digitization of these assets decentralized, safe, trustworthy, and free of a third party.

**There are two forms of digital assets that one can use in NEO:**

* Global Assets.
* Contract Assets.

Global assets are recognized by the whole system and can be identified by all smart contracts and clients.

Contract assets are assets that are only recognized in their specific contracts and cannot be used in other contracts. Eg. GNT the golem token can be used in Golem but it cannot be used in Bancor.

**Neo Blockchain and Digital Identity**

This is how Wikipedia defines Digital Identity:

**A digital identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organisation, application, or device. ISO/IEC 24760-1 defines identity as “set of attributes related to an entity.”**

For digitization of assets to work, it is critical to have trustworthy digital identities.

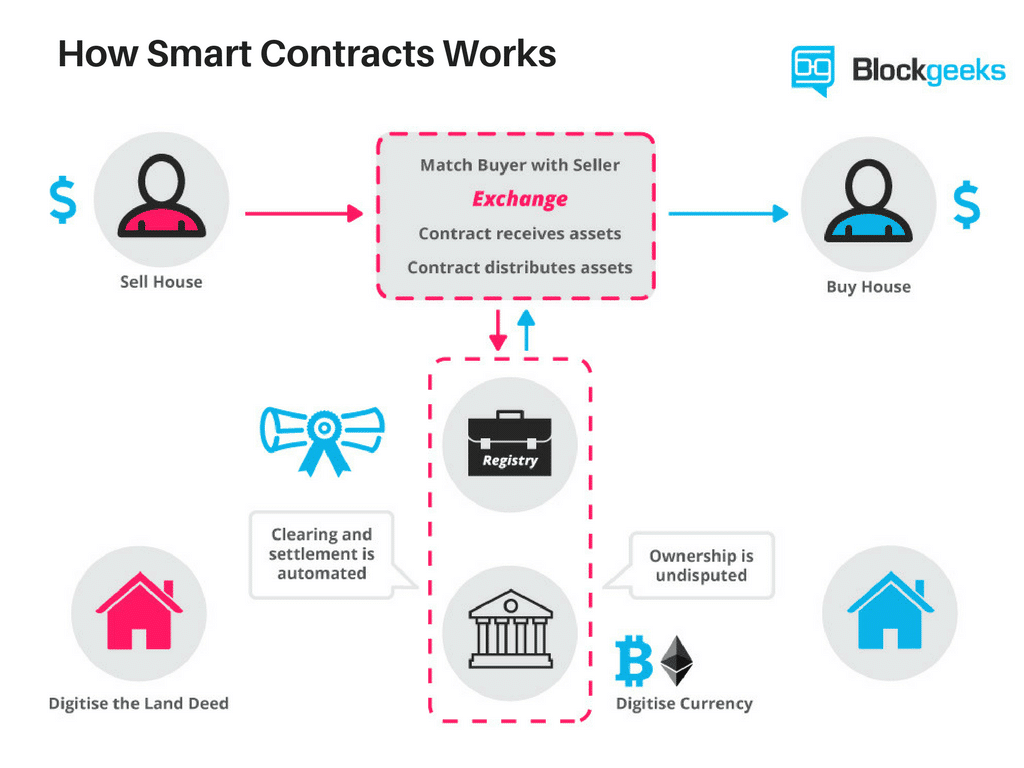
The NEO platforms utilizes the X.509 digital identity standard, the most widely accepted digital certificate issuance model, based on Public Key Infrastructure. Along with the aforementioned X.509 standard., the Web of Trust point-to-point certificate issuance mode, is supported as well.

**Identity verification in NEO will be done by:**

* Use of facial features.
* Fingerprints.
* Voice.
* SMS.
* Other multi-factor methods.

**Smart Contract**

[Smart contracts](https://blockgeeks.com/guides/smart-contracts/)are automated contracts. They are self-executing with specific instructions written on its code which get executed when certain conditions are made.

[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image3.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

You can learn more about smart contracts in [our in-depth guide here.](https://blockgeeks.com/guides/smart-contracts/)

So, what are the desirable properties that we want in our smart contract?

Anything that runs on a blockchain needs to be immutable and must have the ability to run through multiple nodes without compromising on its integrity. As a result of which, smart contract functionality needs to be three things:

* Deterministic
* Terminable.
* Isolated.

**Feature #1: Deterministic**

A program is deterministic if it gives the same output to a given input every single time. Eg. If 3+1 = 4 then 3+1 will ALWAYS be 4 (assuming the same base). So when a program gives the same output to the same set of inputs in different computers, the program is called deterministic.

There are various moments when a program can act in an un-deterministic manner:

* **Calling un-deterministic system functions:** When a programmer calls an un-deterministic function in their program.
* **Un-deterministic data resources:** If a program acquires data during runtime and that data source is un-deterministic then the program becomes un-deterministic. Eg. Suppose a program that acquires the top 10 google searches of a particular query. The list may keep changing.
* **Dynamic Calls:** When a program calls a second program it is called dynamic calling. Since the call target is determined only during execution, it is un-deterministic in nature.

**Feature #2: Terminable**

In mathematical logic, we have an error called “halting problem”. Basically, it states that there is an inability to know whether or not a given program can execute its function in a time limit. In 1936, Alan Turing deduced, using Cantor’s Diagonal Problem, that there is no way to know whether a given program can finish in a time limit or not.

This is obviously a problem with smart contracts because, contracts by definition, must be capable of termination in a given time limit. There are some measures taken to ensure that there is a way to externally “kill” the contract and to not enter into an endless loop which will drain resources:

* **Turing Incompleteness:** A Turing Incomplete blockchain will have limited functionality and not be capable of making jumps and/or loops. Hence they can’t enter an endless loop.
* **Step and Fee Meter:** A program can simply keep track of the number “steps” it has taken, i.e. the number of instructions it has executed, and then terminate once a particular step count has been executed.Another method is the Fee meter. Here the contracts are executed with a pre-paid fee. Every instruction execution requires a particular amount of fee. If the fee spent exceeds the pre-paid fee then the contract is terminated.
* **Timer**: Here a pre-determined timer is kept. If the contract execution exceeds the time-limit then it is externally aborted.

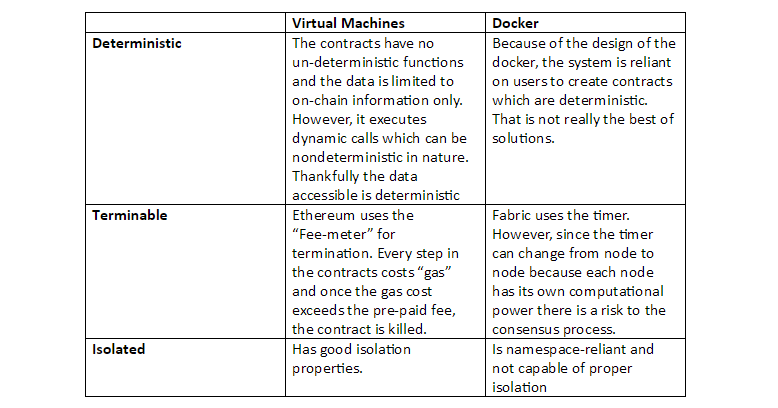
**Feature #3: Isolated**

In a blockchain, anyone and everyone can upload a smart contract. However, because of this the contracts may, knowingly and unknowingly contain virus and bugs. If the contract is not isolated, this may hamper the whole system. Hence, it is critical for a contract to be kept isolated in a sandbox to save the entire ecosystem from any negative effects.

Now that we have seen these features, it is important to know how they are executed. Usually the smart contracts are run using one of the two systems:

* **Virtual Machines:** Ethereum and Neo use this.
* **Docker:** Fabric uses this.

Let’s compare these two and determine which makes for a better ecosystem. For simplicity’s sake, we are going to compare Ethereum (Virtual Machine) to Fabric (Docker).

[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/non.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

So, as can be seen, Virtual Machines provide better Deterministic, terminable and isolated environment for the Smart contracts. However, dockers have one distinct advantage. They provide coding language flexibility.

In a Virtual Machine (VM) like Ethereum, one needs to learn a whole new language (solidity) to create smart contracts.

What the Neo developers aimed to do was to create a Virtual Machine that could give all the advantages of a VM and also give the code-flexibility of a docker.

**Imagine creating a smart contract using Javascript or C#!**

Neo’s solution was Smart Contract 2.0 system which makes it extremely alluring and in-demand. This will be explored later on in the article.

Similarities with Ethereum

It is inevitable that more often than not, in this article we will compare Neo with Ethereum. So before we proceed any further, let’s look at some similarities between the two.

* Both of them provide a platform for developers to create [dAPPS](https://blockgeeks.com/guides/dapps/)and various ICOs on a blockchain.
* Everything in the blockchain runs via the exchange of a crypto-asset. Ether in Ethereum’s case and GAS in Neo’s case.
* Both are Turing complete. A machine that can “calculate anything” given there is unlimited memory space available is called “Turing Complete”. So basically the machine that drives both these projects EVM and NeoVM can solve any problem given it has enough memory space.

So, while there are similarities no doubt, what makes Neo so interesting are its features that make it different from Ethereum. The features that has given it the sensationalistic moniker of “Ethereum Killer”.

**The Two Tokens: NEO vs GAS**

The Neo ecosystem has two tokens:

* NEO – formerly known as Antshares (ANS).
* GAS – formerly known as Antcoins (ANC).

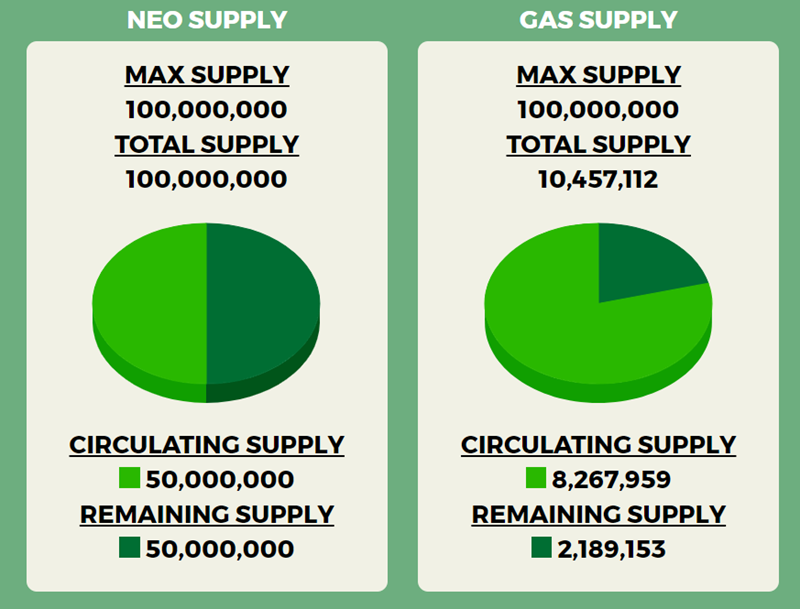
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image2.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: Coinsutra

NEO

[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image5-1.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: Coin Market Cap.

NEO has a total of 100 million tokens.

Ownership of the NEO gives the holder rights to manage and make decisions for the network.  These rights include bookkeeping, NEO network parameter changes etc.

***The NEO token can’t be subdivided into decimals with the least possible unit being 1.***

The 100 million NEO tokens is divided into two portions. The first portion of 50 million tokens was distributed during their ICO.

The second portion is 50 million was locked up for a year (till October 16 2017) and is to be used only for long-term growth and support of NEO projects and for the long-term development, operation, and maintenance of the NEO ecosystem.  The plans for these 50 million tokens is as below:

* 10 million tokens will be used to motivate NEO developers and members of the NEO Council
* 10 million tokens will be used to motivate developers in the NEO ecosystem
* 15 million tokens 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 will be retained as a contingency
* The annual use of NEO in principle shall not exceed 15 million tokens.

**GAS**

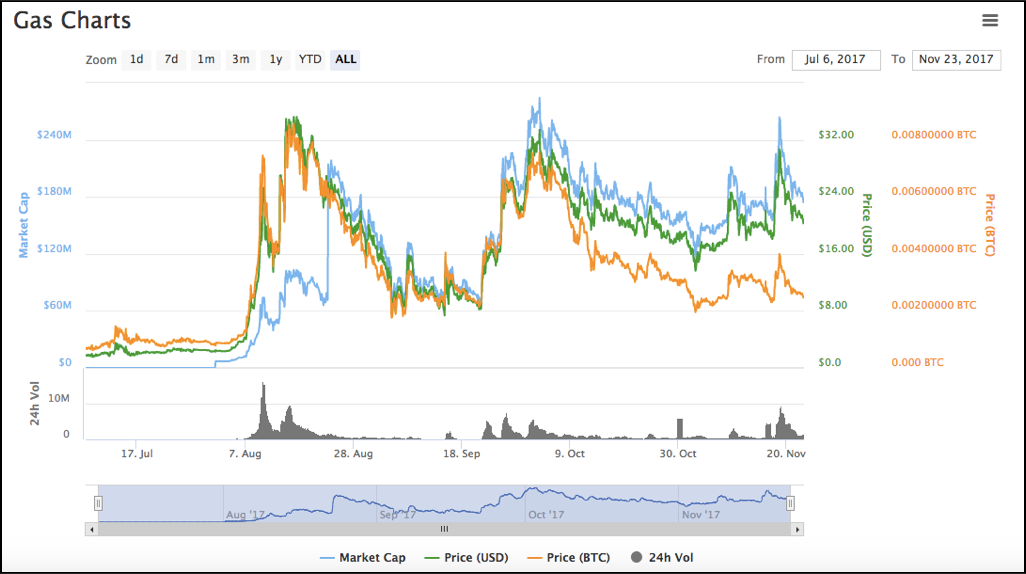
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image4-1.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: Coin Market Cap

If NEO is the token that gives you voting and decision making rights in the community, then GAS is what fuels smart contracts and get things done. It is, as the name states, the fuel of the network. GAS is what will be exchanged as currency inside the ecosystem and it is what is going to economically incentivize the various projects taking place in it.

Quite like NEO it has a total limit of 100 million tokens, however, unlike NEO it is divisible. The minimum unit of GAS is is 0.00000001.

There is another major point of difference between the two.

The 100 million NEOs have already been generated in the genesis block, i.e. the first block of the blockchain, of the NEO network. The 100 million GAS has not yet been generated. They will be generated corresponding to the 100 million NEO via a decay algorithm in about 22 years’ time to the address holding the NEO. If the NEO is transferred to a new address, the GAS generated will be credited to the new address.

2 million blocks will be generated each year with a downtime of around 15-20 seconds between consecutive blocks. The initial GAS generation is going to be 8 GAS per block and that is going to reduce by 1 GAS per year or 1 GAS per 2 million blocks till only 1 GAS is produced per block.  At the 44 millionth block, the total GAS generated will reach 100 million after which there will be no GAS generation.

**According to the algorithm:**

* 16% of the GAS will be created in the first year.
* 52% will be created in the first four years.
* 80% GAS will be created in the first 12 years.

The GAS will be released proportionally in accordance with the NEO holding ratio to the corresponding addresses. The NEO holders can claim these GAS tokens anytime they want. If you want a tool which will calculate how much GAS you are eligible to in accordance the amount of NEO you hold [then you can use this](https://neotogas.com/).

In order to create a better user experience, the NEO network will vote and set a threshold to exempt GAS from a certain amount of transfer transactions and smart contract operations.

If a large number of spam transactions does occur, users with NeoID can get their transactions and smart contract prioritized over the others. If, however, you don’t have a NeoID then you can prioritize your transactions by paying more GAS.

**dBFT Consensus Mechanism**

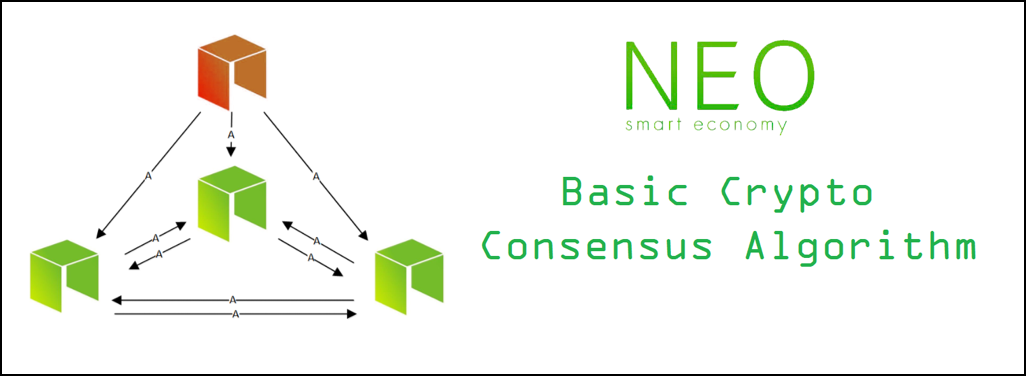
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image7.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: basiccrypto Steemit article

Before we begin, huge shoutout to “basiccrypto” and his Steemit article for the data.

One of the biggest challenges that most distributed systems face is coming to a consensus. This problem is usually called “[Byzantine General’s Problem](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance)”.

**So what is the Byzantine General’s Problem?**

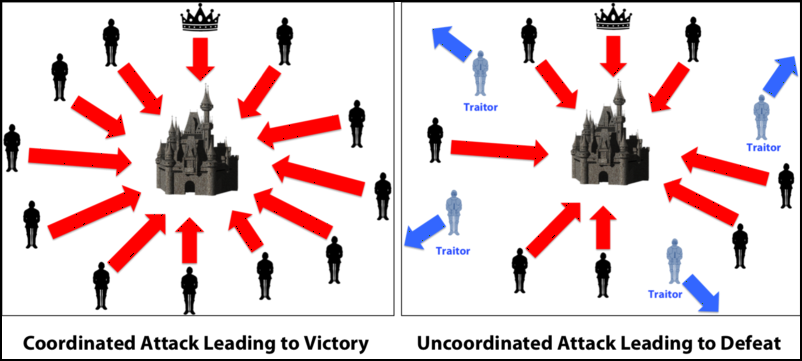
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image6.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: Medium

Ok so imagine that there is a group of Byzantine generals and they want to attack a city. They are facing two very distinct problems:

* The generals and their armies are very far apart so centralized authority is impossible, which makes coordinated attack very tough.
* The city has a huge army and the only way that they can win is if they all attack at once.

In order to make successful coordination, the armies on the left of the castle send a messenger to the armies on the right of the castle with a message that says “ATTACK WEDNESDAY.”

However, suppose the armies on the right are not prepared for the attack and say, “NO. ATTACK FRIDAY” and send back the messenger through the city back to the armies on the left. This is where we face a problem.

A number of things can happen to the poor messenger. He could get captured, compromised, killed and replace with another messenger by the city. This would lead to the armies getting tampered information which may result in an uncoordinated attack and defeat.

This has clear references to blockchain as well. The chain is a huge network; how can you possibly trust them? If you were sending someone 4 Ether from your wallet, how would you know for sure that someone in the network isn’t going to tamper with it and change 4 to 40 Ether?

Satoshi Nakamoto, the creator of [Bitcoin](https://blockgeeks.com/guides/what-is-bitcoin/), was able to bypass the Byzantine General’s problem by inventing the proof of work protocol. This is how it works. Suppose the army on the left want to send a message called “ATTACK MONDAY” to the army on the right, they are going to follow certain steps.

* Firstly, they will append a “nonce” to the original text. The nonce can be any random hexadecimal value.

* After that, they hash the text appended with a nonce and see the result. Suppose, hypothetically speaking, the armies have decided to only share messages which, on hashing, gives a result which starts with 5 zeroes.

* If the hash conditions are satisfied, they will send the messenger with the hash of the message. If not, then they will keep on changing the value of the nonce randomly until they get the desired result. This action is extremely tedious and time-consuming and takes a lot of computation power.

* If the messenger does get caught by the city and the message is tampered with, according to hash function properties, the hash itself will get drastically changed. If the generals on the right side, see that the hashed message is not starting with the required amount of 0s then they can simply call off the attack.

This is the proof-of-work protocol that is used by Bitcoin and Ethereum (as of writing). The problem with that is proof-of-work is extremely wasteful and inefficient energy wise. There are more consensus mechanisms out there of course. Ethereum eg. is planning to move to Proof of Stake [soon via the implementation of Casper](https://blockgeeks.com/guides/ethereum-casper/).

However, Neo has decided to use a interesting kind of consensus mechanism system which, they believe, is going to help them scale better. It is called Delegated Byzantine Fault Tolerance OR dBFT. Let’s see how it works.

**What is dBFT?**

Imagine that there is a country “Blockgeeks” and this country has a lot of citizens. Each of these citizens would elect a Delegate to represent them and to make them happy. The job of these delegates is to pass laws that will make the citizens happy, if they are not good at their job then the citizens can simply vote for another delegate the next time.

So how do the delegates pass laws?

One of the delegates is randomly chosen as a speaker.

The Speaker then look at all the demands of the citizens and creates a law. They then calculate a “Happiness Factor” of these laws to see if the number is enough to satisfy the citizen’s needs or not. They then pass that down to the delegates.

The delegates then individually check the Speaker’s calculations. If the the speaker’s number matches the Delegate’s then they give their approval, if not then they give their disapproval.

66% of the delegates need to give their approval for the law to pass. If the majority is not sealed, then a new leader is chosen and the process starts again.

**So, let’s see how this applies in the blockchain.**

The citizens are whoever owns NEO tokens aka ordinary nodes.

Delegates are the bookkeeping nodes. In order to be a bookkeeping node you need to satisfy a certain amount of qualifications: having special equipment, dedicated internet connections and a certain amount of GAS (1000 according to basiccrypto’s article).

* The “demands of the citizens” are basically the various transactions made by the token holders.
* The “law” is the current block that is to be added to the blockchain.
* The “happiness factor” is the hash of the current block.

Now, there are two cases where one of the participants may act in a malicious manner. Let’s check it out:

**Case #1: The Speaker is malicious**

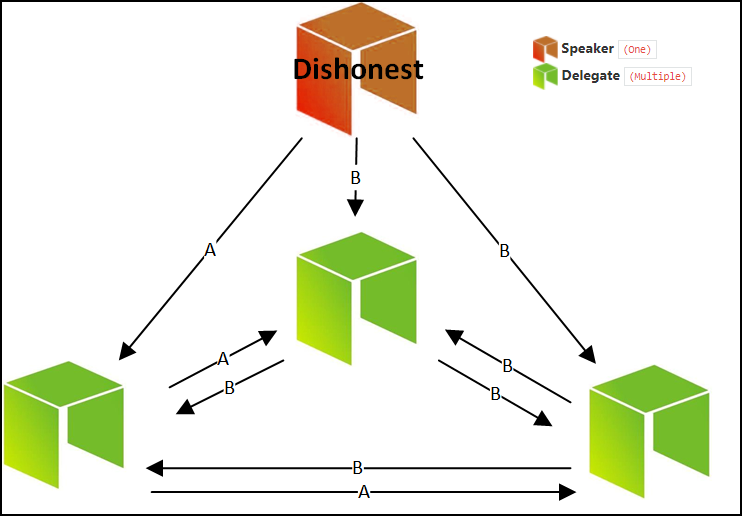
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image9.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image credit: basiccrypto Steemit article

In this case, the speaker has sent a malicious message B to two delegates and an accurate message to one.  This scenario can be easily mitigated because of the majority rule. The two delegates will see that their hash is not matching up with that of the speaker while one delegate will see that their hash matches up perfectly. However, 2 out of 3 will disapprove the proposal and consensus won’t be reached. The speaker will henceforth be removed.

**Case 2: One of the delegates is malicious**

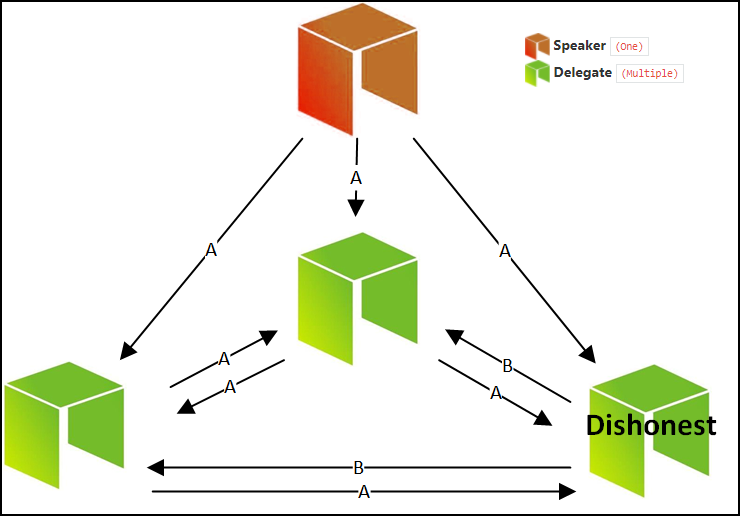
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image8.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image credit: basiccrypto Steemit article

The speaker sends the correct message to all the delegates, however, one of the delegates decides to act in a malicious manner and declares that their number isn’t matching up with the speakers. However, as can be seen, since 2 out of the 3 delegates are non-malicious, they will approve the law which will then be passed since a 66% consensus has been reached.

So as can be seen, dBFT presents a very interesting form of consensus mechanism.

**NeoContract: The Smart Contract 2.0**

As we have mentioned before, Neo’s aim was to bring in all the advantages of a Virtual Machine along with the flexibility of coding languages. Let’s see how they managed to accomplish that.

**Neo’s smart contract system has three parts to it:**

* NeoVM.
* InteropService
* DevPack

**NeoVm**

This is a pictorial representation of the Neo Virtual Machine:

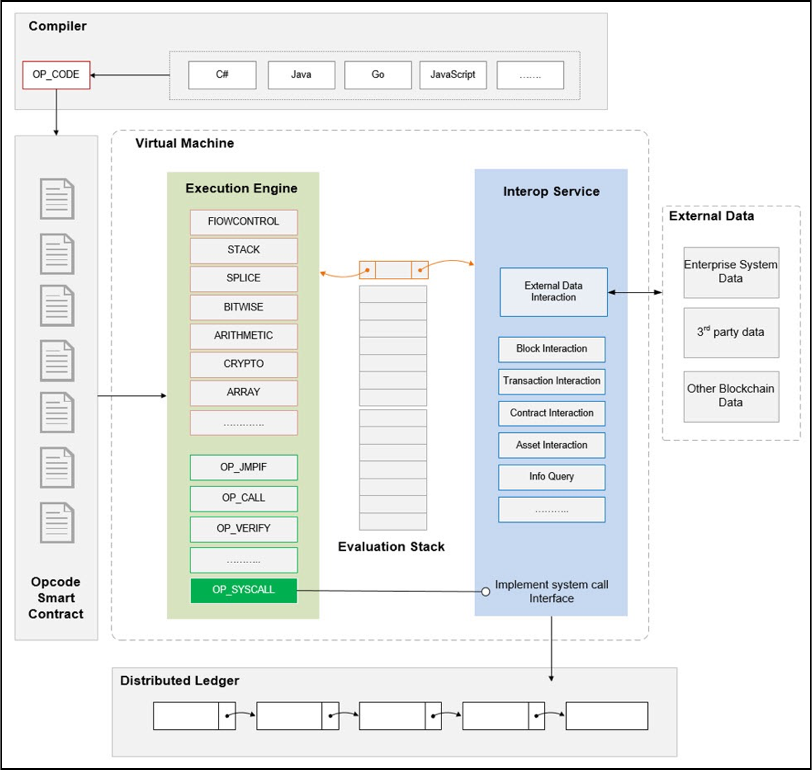
[Save](http://pinterest.com/pin/create/bookmarklet/?media=https://blockgeeks.com/wp-content/uploads/2017/12/image10.png&url=https://blockgeeks.com/guides/neo-blockchain/&is_video=false&description=What%20is%20Neo%20Blockchain%3F%20Beginners%20Guide%20)

Image Credit: Neo Whitepaper

As the Neo Whitepaper states, the NeoVM or Neo Virtual Machine is a lightweight, general-purpose VM whose architecture closely resembles JVM and .NET Runtime. It is 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 is versatile with a good start-up speed which makes it a great environment to run smart contracts.

**InteropService**

The InteropService increases the utility of the smart contracts. It allows the contracts to access data outside the NeoVM without compromising on the overall stability and efficiency of the system.

Currently, the interoperable service layer provides some APIs for accessing the chain-chain data of the smart contract. The data that it can access are:

* Block information.
* Transaction information
* Contract information.
* Asset information

….among others.

It also provides storage space for smart contracts.

**DevPack**

DevPack includes the high-level language compiler and the IDE plug-in. Since the NeoVM architecture is pretty similar to JVM and .NET Runtime, it enables contracts to be coded in other languages. As you can imagine, this greatly reduced the time taken by developers to learn how to create smart contracts.

**Future features of Neo**

Shoutout to @jeremylqe’s article “Neo Wiki” for the following data.

* **NeoX:** Will enable cross-chain interoperability.

* NeoFS**:** It is a file storage protocol that uses distributed hash table technology. It indexes file by utilizing the hash of its content rather than the file path. Large files will be divided into fixed-size data blocks and distributed and stored in various nodes.

* **NeoQS:** NeoQS (Quantum Safe) is a lattice-based cryptographic mechanism. Quantum computing poses a genuine threat to [cryptographic systems based on RSA and ECC.](https://blockgeeks.com/guides/cryptocurrencies-cryptography/) This means that Ethereum and Bitcoin, both of which utilize ECC, are potentially at risk of being hacked by quantum computing. Neo is looking to address that issue via NeoQS.

**Where can I buy and store NEO?**

Big shoutout to Coinsutra for the following data.

You can buy Neo in the following exchanges:

* Binance
* Bittrex
* Yumbi
* Jubi
* Yuanbao
* 19800
* Yobtc
* Cryptopia

And if you are looking for wallets to store your Neo then you can use the following:

* [Hardware wallet: Ledger Nano S.](https://www.ledgerwallet.com/r/eb7e)
* Desktop wallet: NEON.
* Web wallet: Neo tracker.
* Paper Wallet: Ansy.

You can learn more details about [storing Neo in wallets here.](https://coinsutra.com/best-neo-wallets/)

**What is the future of Neo?**

So how is the future looking for the “Ethereum killer”?

It is too soon to say whether it can live up to the moniker or not, but the biggest advantage that it has over Ethereum is the relatively low barrier to entry. Since the developers don’t have to learn a new language to create smart contracts it can definitely look appealing. How it fleshes out in the future remains to be seen. However, Neo is backed the Chinese government and bigshots like WINGS and Alibaba.

We are not sure whether it will “kill” Ethereum or not, but what we do know is that it presents an amazing platform for developers to add to the ever-expanding cryptosphere.