EPOCHTOKEN WHITEPAPER V2.0

Decentralized and non-profit Ecosystem platform.

April 10, 2021

Abstract

When you use traditional payment methods, you need to rely on a third party to set up your transaction. They keep their own private records that store the transaction history and balance of each account. Proof of stake is a type of consensus mechanism used by blockchain networks to achieve distributed consensus. The purpose of this article is to explain to system reimbursement partners the awards they have earned by producing on Eph Stake. You will find out how Epochtoken works in this article.

Proof-of-Stake

Proof of Stake is a consensus algorithm whereby new blocks are secured by validators before being added to the blockchain. In proof of stake mining algorithm, a person (node) can participate in the mining process by "staking" a given amount of their coins to be allowed to validate a new transaction.

The PoS is a deterministic concept that simply states that an individual is only able to mine or validate new blocks equivalent to the number of coins they possess in their staking account. It implies that the more coins you have, the higher your mining power, i.e., the more coins you have in your wallet, the more transactions you can validate to earn block rewards.

Proof of stake will make the consensus mechanism completely virtual. While the overall process remains the same as proof of work (POW), the method of reaching the end goal is entirely different. In POW, the miners solve cryptographically hard puzzles by using their computational resources.

The chosen validators then stake the required amount of coins using the special staking wallets. The node will forge or create new blocks proportional to the number of coins in their wallets. For instance, if you have 1% of all the coins, then you can "mine" 1% of the new blocks.

Benefits of a PoS consensus system..

- *Proof of Stake consensus mechanism doesn't require specialized and expensive hardware to run. You only need an internet connection and a functional computer setup.*
- *Anyone with enough coins to stake can validate transactions on the network.*
- *Investments in a PoS system do not depreciate with time like what happens to ASICs, GPU and other mining hardware. A validators' initial stake can only be affected by price fluctuations and trading rates.*

  Proof of Stake is more energy efficient and environmentally friendly than Proof of Work regarding power consumption.
- Reduced threat of 51% attack.
- Block confirmations are very fast.

Masternode Rewards

A wallet can perform block verification for every coin it has over 10000 epochtoken. The wallet system is instantly connected to the transfers pool via the websocket. Among the connected nodes, the system generates hash on the node it chooses depending on the coin amount and informs the other nodes.

In order to be selected for the node pool, the peer registered node must remain connected to the system for 7 days with 99.99% uptime.

Users in the epochtoken ecosystem can stake through the system whenever they want via They can earn staking income through these token's that are epoch without paying any additional expense like server internet uptime.

Coin Supply

150.000.000 Epochtoken reserved for the development of the project by developers to sell on ico.
The remaining 9,850,000,000 epoch tokens have been left to the control of the community involved in the project

Proof-of-Stake Pool

Epochtoken offers users a private wallet gateway service. In this wallet system, through internal wallets connected to the main node, users can earn staking income without paying any additional server cost.

On the Epochtoken, 10,000,000.000 million tokens in the main wallet were created and transferred on the first block so that all users could stake more easily and quickly. These coins are used in the first transfers. The 9.850.000.000 epochtoken that will be formed as a result of the figing of the blocks are distributed daily as staking, and partnership income.

Every user staked via vault will receive coins daily with none of cost like server and wallet. All coins in the vault are stored on cold wallets.

Block Generation under Proof-of-Stake

In order to earn or generate tokens with the Proof of Stake system, Epoch wallet have to deposit some coins to his/her account. So if you have "0" (zero) coins in your account, you cannot earn reward via Proof of Stake.

If you have tokens in your account, all you have to do is wait. There is no minimum waiting period for coins using Proof of Stake is instant same blocks. So you can start earning rewards from a in a moment the coin is first loaded into your wallet.

For the Epochtoken this process ultra fast. When you stake your tokens in stake system you will start earning

Elliptic Curve Cryptography (ECC)

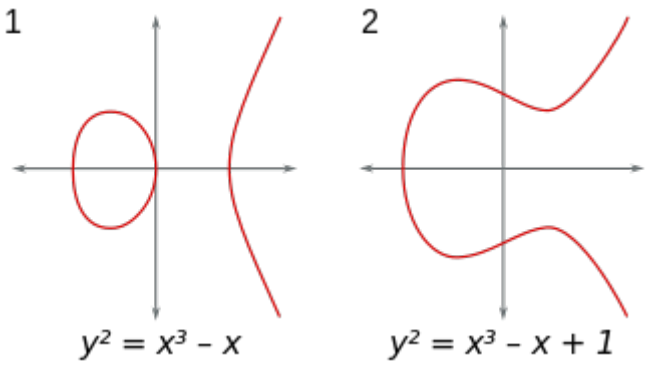
In 1985, cryptography based on elliptic curves was proposed independently by Neal Koblitz and Victor Miller.

In the cryptographic usage, the same ideas of finding two unique numbers (points in a two dimensional curve) which are related and a max ceiling to wrap around apply.

Elliptic curves have some curious characteristics that make them useful. They are defined as a curve that is completely smooth (*non-singular*) and a line between two points on this curve will always intersect a third point (*projective*). This allows you to quickly hop around this curve easily (computationally) and procedurally come up with an endpoint that has seemingly no relation to the starting point and is very difficult to reverse the path that led you there.

Elliptic Curve Cryptography is an approach to public-key cryptography, based on elliptic curve area (Kapoor, Abraham, & Singh, 2008), In principle, ECC is an algorithm in which each side has a pair of private key and public key. The private key is only held by special parties, while the public key is distributed to all parties. Elliptic Curve Cryptography based on the algebraic structure of the elliptical curve on a finite area.

$$y^2 = x^3 + ax + b$$



Graphs of curves $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$

Elliptic Curve Cryptography (ECC) has some advantages when compared to other asymmetric cryptography that is in terms of bit key length is shorter but has the same level of security. In comparison, the 160-bit Elliptic Curve Cryptography has a security level (08/03/1010 MIPS / Million Instructions per Second year) which is equal to 1024 bit RSA has a security level (3.1012 MIPS year).

Elliptic Curve Digital Signature Algorithm (ECDSA)

Epochtoken uses the Elliptic Curve Digital Signature Algorithm (ECDSA) based on elliptic curve cryptography. The particular elliptic curve is known as secp256k1, which is the curve

$$y^2 = x^3 + 7 \pmod{p}$$

The idea is to take the equations motivated by the geometry in the plane then use those equations to define addition when you're not working over real numbers but over a different field. In the case of secp256k1, the field is the finite field of integers mod *p* where

$$p = 2^{256} - 2^{32} - 977$$

Here *p* was chosen to be relatively close to 2^{256}. It's not the largest prime less than 2^{256}; there are a lot of primes between *p* and 2^{256}. Other factors also went into the choice *p*. Note that we're not working in the integers mod *p* per se; we're working in an Abelian group whose addition law is defined by an elliptic curve over the integers mod *p*.

The best algorithms for solving discrete logarithm problems in a group of size *n* currently require $O(\sqrt{n})$ operations. How big is *n* in our case?

The base point *g* was chosen to have a large order, and in fact its order is approximately 2^{256}. Specifically, the order of *g* written in hexadecimal is

n = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141.

This means that we get approximately 256/2 = 128 bits of security because $\sqrt{(2^{256})} = 2^{128}$

Masternodes

- It requires 10.000 Epoch token to be left unusable by the holder to remain functioning as a masternode.
- It must be left connected at all times.
- Requires a separate IP address to the wallet of the intended user.

* Note Some aspects of the setting up of a masternode can be complicated for less technically-minded users.

These lack of freedoms mean that if the reward were to be identical to staking, the likelihood of anyone choosing to host a masternode would be significantly lower.

With that said, there are advantages to staking over hosting a masternode. These include:

- The ability to opt in and out of staking as the user pleases.
- No requirements on specific denomination.

There are validators in POS instead of miners. Validators lock some of their Epochtoken as a share in the ecosystem. Following this, validators place a Stake on the blocks they think will be added next to the chain. When the block is added, validators receive a block reward proportional to their share.

Block Signatures and Duplicate Stake Protocol

CryptoJS

CryptoJS is a growing collection of standard and secure cryptographic algorithms implemented in JavaScript using best practices and patterns. They are fast, and they have a consistent and simple interface.

Although the PoS consensus algorithm indeed does sound great, there is one disadvantage and that is that decentralisation is not fully possible.

This is because staking can still be monopolized by a few of the nodes on the network. Those that have the most coins can effectively control most of the mining.

HASH Algorithm

What is hashing? In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string through SHA-256 hashing.

In cryptographic hashing, the hashed data is modified in a way that makes it completely unreadable. It would be virtually impossible to convert the 256-bit hash mentioned above back to its original 512-bit form. So why would you want to create a scrambled message that can't be recovered? The most common reason is to verify the content of data that must be kept secret. For example, hashing is used to verify the integrity of secure messages and files. The hash code of a secure file can be posted publicly so users who download the file can confirm they have an authentic version without the contents of the file being revealed. Hashes are similarly used to verify digital signatures.

SHA-256

SHA-256 is one of the four variants in the SHA-2 set. It isn't as widely used as SHA-1, though it appears to provide much better security. The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

SHA-512

SHA-512 is largely identical to SHA-256 but operates on 64-bit words rather than 32.

EPOCHTOKEN DETAILS

Min Stake : 10,000 Epochtoken

Daily Stake Earnings : 90days/12% monthly - 180days/16% monthly - 360days/20% monthly

Decrease in staking rates: There will be 1% decrease after every 3 months

Epochtoken withdrawal fee : %3 or %2 tron(Trx)

Epochtoken marketing plan: You will have a share of 15% of total of 3 depths.

The infrastructure it is in: Tronchain(trc10)

Block Difficulty Adjustment Interval : Retarget every block

Genesis Block Difficulty : 0

Block Size : 1 TB Max

Max Transactions : >4000 (CPU Bond)

Energy Efficient : Yes CPU Optimal

Total Supply : 10,000,000.000.00000000

Decimals : 8

Token ID : 1004025

ICO SALE : EPH tokens received in ico sale will be automatically locked for 1 year.

EPOCH TOKEN

In conjunction with our solution partners within the global ecosystem of Epoch token, we offer our potential investors, traders a strategy consisting of multiple platforms to provide more revenue, tremendous benefits, and dedicated application opportunities. With this strategy, we will offer our traders more sales, more customers, more advertising opportunities. We will offer our potential investors and users more space to use Epoch token within the Epoch ecosystem. EPOCH is a lucrative project for everyone. It is designed as a solution that you can both earn and earn while responding to different needs and different types of communities. **It is the community within the real owners of the Epochtoken project.**