**What Is a Consensus Mechanism?**

A consensus mechanism is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things.

**Consensus means achieving a state of a decision on which all network participants agree.** For example, a group of friends decides on a trip to Goa without conflicts. Here, reaching a decision to visit Goa together is a state of consensus or mutual agreement.

**“The purpose of the Consensus mechanism in a decentralized network is to allow a group of independent nodes to distribute the right to update as well as validate the change in the network equally..”**

* A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network.
* In the context of blockchains and cryptocurrencies, proof-of-work (PoW) and proof-of-stake (PoS) are two of the most prevalent consensus mechanisms.
* Critics of Bitcoin miners have argued that PoW is overly energy-intensive, which has sparked the creation of new and more efficient mechanisms.

**Pros Explained**

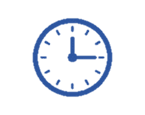
* **Forms agreement foundational to the crypto-market**: Consensus mechanisms synchronize data between all participating users and enable trust in a blockchain.
* **Creates a secure environment**: Cryptocurrencies and distributed applications rely on consensus mechanisms for security.
* **Anyone can participate**: With the most popular consensus mechanisms, barriers to participating as a miner or operating their own nodes are not very high.

**Cons Explained**

* **May be energy-intensive**: Proof-of-work is extremely energy-intensive and requires as much electricity as many countries.11
* **Potential for attacks**: There’s a small chance for a type of hack called a 51% attack, among other minor weaknesses.

**Various consensus algorithms and how they work**:  
  


**Proof of Elapsed Time**



* Proof of elapsed time (PoET) is a consensus algorithm developed by Intel Corporation that enables permissioned blockchain networks to determine who creates the next block.
* PoET follows a lottery system that spreads the chances of winning equally across network participants, giving every node the same chance.
* The PoET algorithm generates a random wait time for each node in the blockchain network; each node must sleep for that duration.
* The node with the shortest wait time will wake up first and win the block, thus being allowed to commit a new block to the blockchain.
* **Blockchain using PoET algorithm:**Hyperledger Sawtooth

The Proof of Elapsed time in blockchain needs to ensure 3 significant factors for this process to work:

* Ensure that the node or network participant **gets the random waiting time** indeed.
* Check if they are**not choosing the shortest waiting time on purpose**.
* Verify if the node has**completed the given waiting time** or not

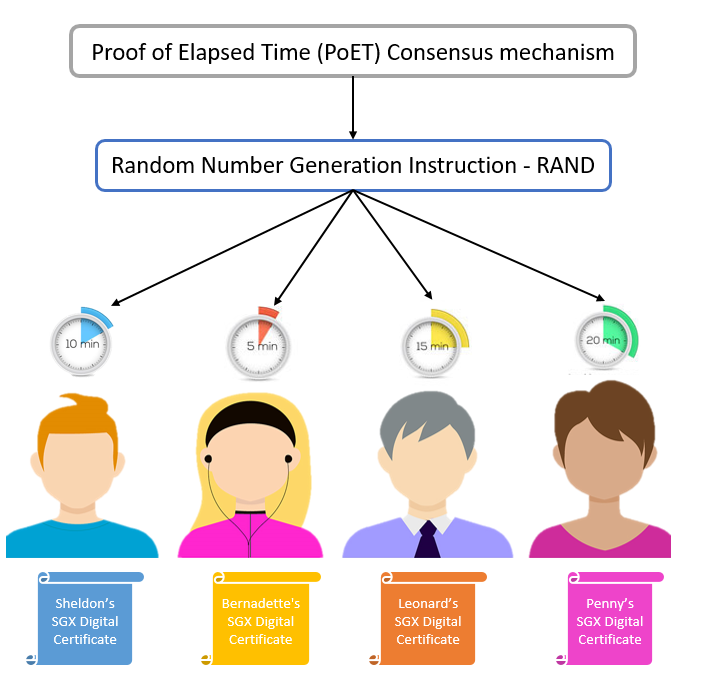
**How does the Proof of Elapsed Time (PoET) Algorithm work?**

Let’s break down the process more accurately into steps.

1. Selection Process
2. Generation Process

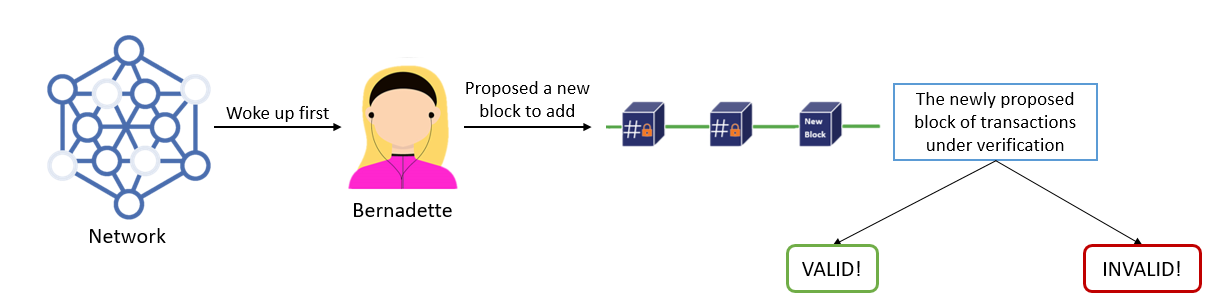
**Selection Process**

* First, each participating node has to share its **certificate by Intel Software Guard Extension (SGX)**, which ensures its validity to generate a new block in the network. After that, they are eligible to get a timer object.
* The numbers assigned to each node as a **timer object** (waiting countdown time) by Intel’s random number generation instruction, RNGI. It generates difficult to detect random numbers. Now, the time object given to each participating node activates.



**Generation Process**

* After the time object ends and the node wakes up, it’s eligible to forge a new block to the network.
* The active node generates the hash (using a hash function like SHA-256) of its block of transactions and submits it for acceptance. It doesn’t require showing computation work done by the node. Afterward, the update gets flooded to the network.



**Benefits of Proof of Elapsed Time (PoET)**

Following are the advantages of the PoET consensus mechanism:

* PoET can go up to **a million transactions per second**.
* It is **highly energy-efficient** and easily scalable.
* It ensures the**same opportunity for network participants** with time object and activation.
* As it’s a permissioned blockchain network, the process of selecting validators **ensures network security**against cyber attacks.

**Limitations of Proof of Elapsed Time (PoET)**

Following are the disadvantages of the PoET consensus mechanism:

* PoET is a**permissioned and closed network**, unlike Bitcoin and Ethereum.
* The mechanism **highly depends on tools by Intel** technology which might raise compatibility issues with other tools later.

**X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X**

**Proof of Authority (PoA)**

****

PoA consensus mechanism was tossed by the co-founder of Ethereum, **Gavin Wood**, in 2017. PoA is an improvisation on the Proof of Stake (PoS) mechanism

Proof of Authority (PoA) is a **reputation-based consensus mechanism** that provides **high performance and fault tolerance**. In similarity with PoS(proof of stake ), PoA also uses the concept of digital signing to verify participant identities. However, PoA asks for **network participants’ reputations at stake**instead of staking coins.

With the PoA algorithm, each miner (or network participant who wishes to add their new block of transactions) has to**prove their reputation and authority** on the network. Hence, **PoA leverages the value of identities** in a private network.

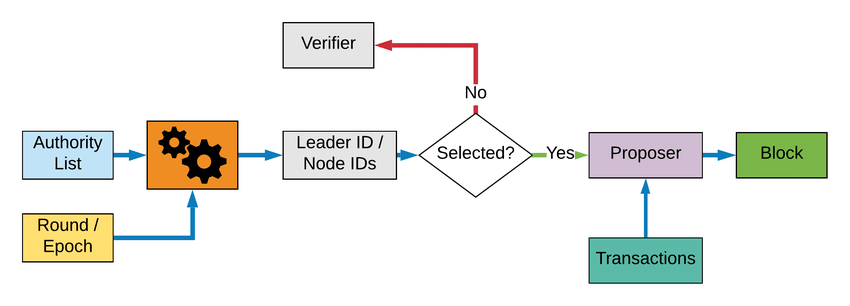
As this mechanism requires almost no computing power, it is far less resource-intensive than some of its predecessors, in particular PoW. It is also one of the less costly options, making it a heavily favoured solution for private networks, such as JP Morgan (JPMCoin). Other PoA-based projects include VeChain (VET) and Ethereum Kovan testnet.

**How can a node become a validator in the PoA mechanism?**

* Verified, valid, and trustworthy network identity
* No criminal record
* Good moral standards
* Stay committed to the network
* Willing to put reputation at stake

**How does the PoA Algorithm work?**

PoA provides the right to generate a new block to those nodes who have proven their authority with reference to their identity in the network. Here, nodes eligible to create a new block are known as **Validators**.



The process of selecting validators requires a lot of verification. Hence, it’s hard to become a validator with PoA consensus.

The **validators are the authenticated miners of the network**. There are a limited number of block validators which makes the system highly scalable. The blocks of transactions are verified and approved by pre-approved network participants who serve as**moderators**.

Here, blocksgeneratein a predictable sequence concerning the number of validators and their reputation in the network**.**

**Benefits of Proof of Authority (PoA)**

* PoA consumes less time and energy compared to PoW and PoS.
* It possesses a greater speed of validating transactions. Hence, a higher transaction rate.
* PoA supports a limited number of validators which makes it highly scalable.
* Assured protection against 51% attacks on the network.
* PoA is a great choice of permissioned or private blockchain networks.

**Limitations of Proof of Authority (PoA)**

* The system is **highly dependent on validators**. Hence, they need to be picked consciously, not randomly.
* It is**not preferred for public networks** or permissionless blockchains.
* PoA consensus algorithm is **less decentralized** in comparison to other algorithms.
* As reward collection in a public network is visible to everyone, it’s**easy to predict the balance of an account** which makes it less secure.
* The mechanism automatically filters out the non-active or non-committed validators, which makes **participants less interested** in the process.
* It’s also pretty **hard to become a validator** on a permissioned network

**X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X**

**Delegated Proof of Stake**

Delegated Proof of Stake (DPoS) mechanism, the **validators’ or delegates’** selection is based on voting. It’s an **additional layer to PoS protocol**. It works similarly to the real-life election and voting system.

DPoS was coined in 2014 by an American cryptocurrency entrepreneur and software developer, **Daniel Larimer**. The DPoS maintains an election process where a selected number of delegates (or validators) are chosen. Those delegates are responsible and trusted by the network participants for validating each new block added to the network.

Users of the network ‘vote’ to select ‘witnesses’ (also known as ‘block producers’) to secure the network on their behalf. Only the top tier of witnesses (those with the most votes) earn the right to validate blockchain transactions.

Besides validating transactions, delegates also help maintain the integrity, reliability and transparency of the blockchain network. The voting power of each delegate is proportional to the number of coins held. They receive rewards for their work with transaction fees, which are shared with their respective electors.

The DPoS algorithm's voting system, and therefore the consensus mechanism, depends on the reputation of the delegates. It's a more scalable mechanism than PoW or PoS since it can process more transactions per second and provide faster confirmation times.

Witnesses in the top tier are always at risk of being replaced by those deemed more trustworthy and who therefore get more votes. They can even be voted out if they fail to fulfil their responsibilities or try to validate fraudulent transactions. This helps to incentivise witnesses to remain honest at all times, ensuring the integrity of the blockchain.

In Delegated Proof of Stake process, users can stake their coins and vote for a particular number of delegates. The weight of a user’s vote is based on their stake. For instance, if a user ‘X’ stakes 20 coins for a delegate and another user ‘Y’ stakes 2, then X’s vote will have more weight compared to that of Y. The delegate that receives the highest number of votes gets a chance to produce new blocks. Delegates get rewarded with transaction fees or a specific amount of coins just like other blockchain consensus mechanisms such as Proof of Stake.

Though less prevalent than PoS, DPoS is regarded by many as being more efficient, democratic, and financially inclusive than its predecessor. It is used by Lisk (LSK), EOS.IO (EOS), Steem (STEEM), BitShares (BTS), and Ark (ARK).

**How does the Delegated Proof-of-Stake Algorithm work?**

This digital democratic consensus algorithm chooses a number of **delegates** (generally, between 21-101, depending on the network strength) by the process of election. **Network participants (or network stakeholders)** vote for their trusted delegate for the network.

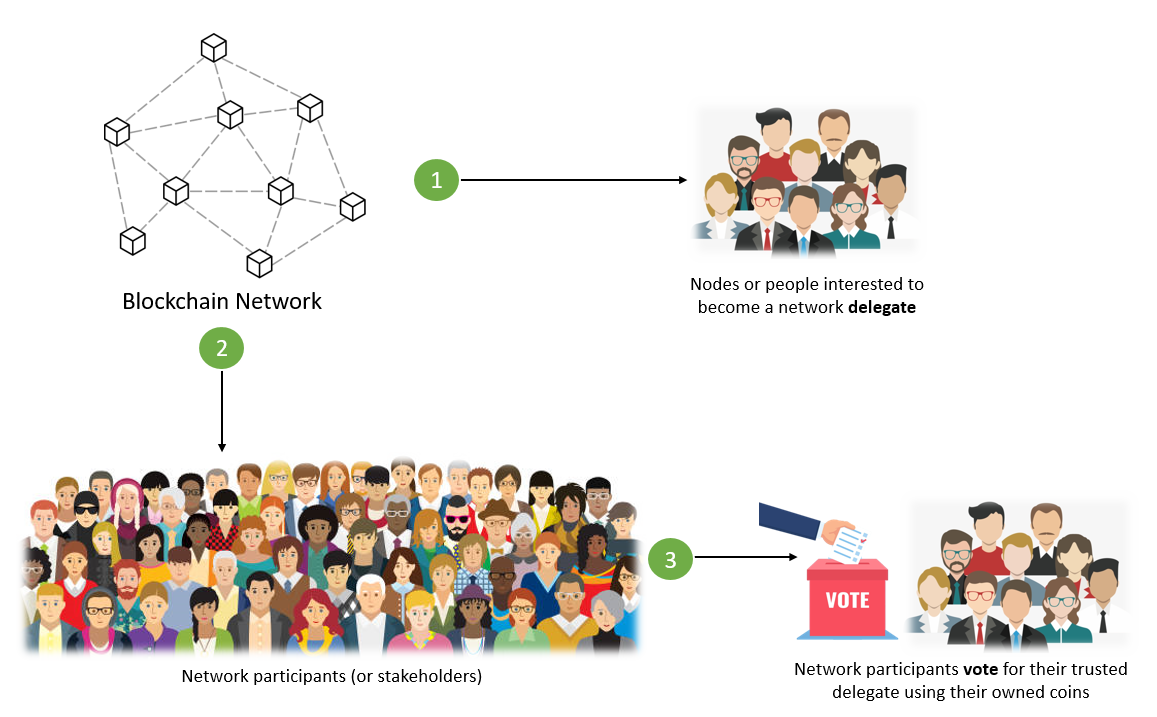
**Role of Delegates (or Witness):**

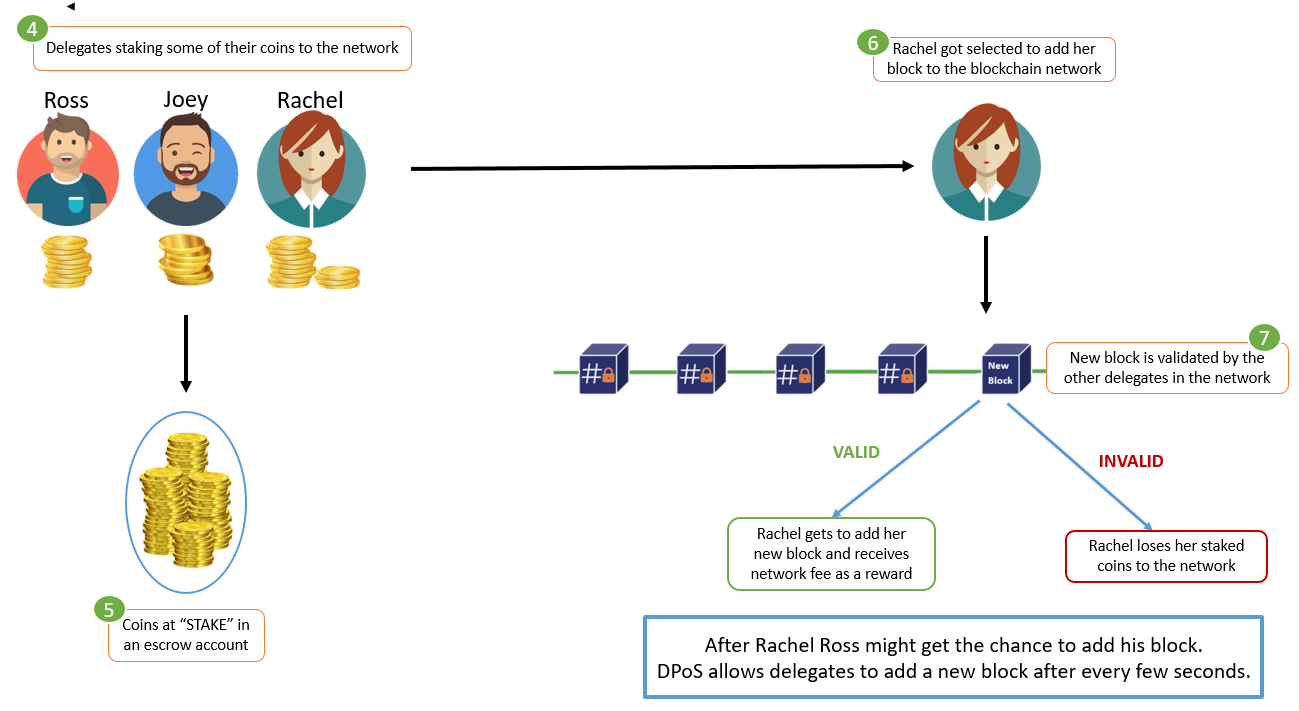
* The selected delegates (or witnesses) validates the transactions of the adding block.
* A delegate can also create his/her own block of transactions to add to the network.
* Delegates receive the rewards for effectively validating other blocks or adding a valid new block.

**Points to remember before Voting:**

* Network participants vote using their coins or tokens.
* Each network participant (or stakeholder) gets the same number of votes as their owned number of coins.
* The stakeholder can also transfer coins to another stakeholder to vote on his/her behalf.

**Note:** Giving votes using coins doesn’t mean voters are giving their coins to the delegates. They are just allotting funds to express their votes. They can reassign their token or coins to vote for some other delegate as well.





Under normal regulated conditions, each delegate produces a block after every few seconds by turns. Each delegate follows the **scheduled time slot** to submit their block.

In case any **delegate shows malicious behavior** or fails to approve his block as valid, loses his reputation and stakes to the network. In addition, that delegate gets immediately replaced by another delegate to keep the process going on. Therefore, DPoS is way faster than the Proof of Work mechanism.

The **blockchains using DPoS** as their consensus mechanism are **EOS** and **Steemit** with 21 witnesses; **Tron** with 27 witnesses; **Cosmos, Bitshare**, and **Lisk** with around 100 witnesses.

**Benefits of Delegated Proof-of-Stake (DPoS)**

Following are the advantages of the DPoS consensus algorithm:

* It **produces limited incentives** for network witnesses as rewards.
* It has a **higher transaction volume** and way **lesser confirmation time**.
* **Time and energy-efficient** protocol.
* **More scalable** as it doesn’t rely on the computing powers of a node or system.
* It provides more power in the hands of network participants. Hence, it encourages a **democratic model**.

**Limitations of Delegated Proof-of-Stake (DPoS)**

Following are the disadvantages of the DPoS consensus algorithm:

* It’s **not applicable to the initial consensus system**. It requires a significant amount of pre-existing participants in the network.
* With a limited number of witnesses, **DPoS can turn the network into centralized**control.
* Delegates should be honest and well-informed about the network progress, which is **hard to find** and struggles with the risk of discrepancy.
* DPoS system can **discourage beginner network participants** with lower coins in the voting process.

**X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X**

**What is Proof of Importance (PoI)?**

The PoI consensus algorithm was introduced by the NEM (New Economy Movement) blockchain in 2015 to overcome the drawbacks of PoS. Their cryptocurrency coin is called XEM.

**Proof of Importance in blockchain resolves the limitations of PoS by assigning consensus addresses and importance scores.** Think of importance scores as a trust or reputation score in the network. A higher score means the network trusts you more to verify or forge the new block of transactions. Hence, higher chances of getting selected as **block harvester** (miners in PoI mechanism).

**With PoI, your chances of verifying the transaction ain’t solely dependent on your stakes. However, it depends on how many transactions and the quality of the transactions you have processed in the past.**

**

Below are the conditions a network participant needs to meet for harvesting a block.

Scale-up the importance score by **vested stake**:

* PoI only counts the vested stakecoins**.**In order to become a vested stake, coins need to be held for a number of days in an account.
* After every 24 hours, 10% of the current unvested amount adds as a vested stake.
* The importance score is directly proportional to the vested stake coins.
* In the case of NEM Blockchain, the block harvester needs to have at least 10,000 XEM called as a **minimum vested stake**.

Elevate the importance score by **making regular and quality transactions**:

* PoI incentivizes nodes that make regular transactions instead of just holding the coins. It promotes the circulation of cryptocurrency among transaction partners.
* Fraudulent transactions just to increase the importance score get detected and will be eliminated by the network.
* PoI provides the importance score to certain types of transactions. Such as, higher transactions get more scores compared to lower transactions.
* In the case of the NEM blockchain, an account has to make the transaction of at least 1000 XEM in the last 30 days to the quality accounts that have at least 10,000 XEM at a vested stake.

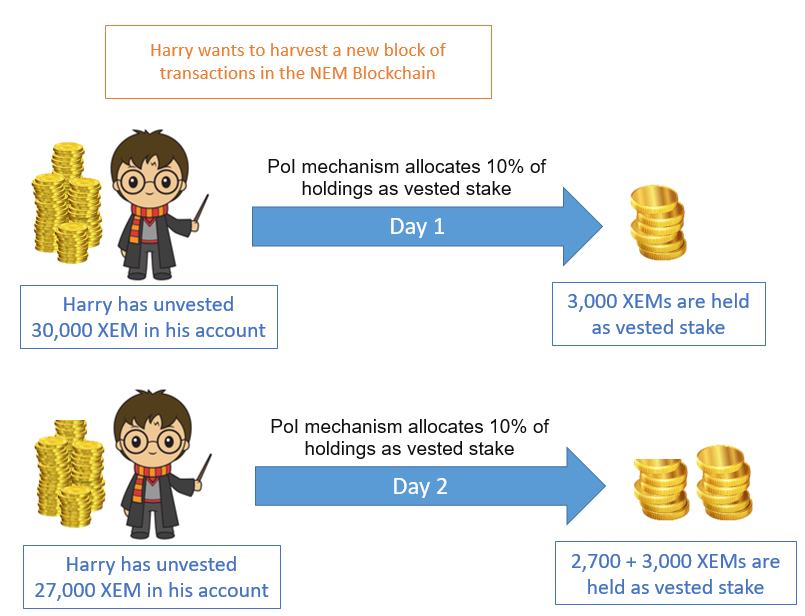
Hence, the importance score depends on factors such as the number of vested coins, transaction partners, the number and size of transactions.

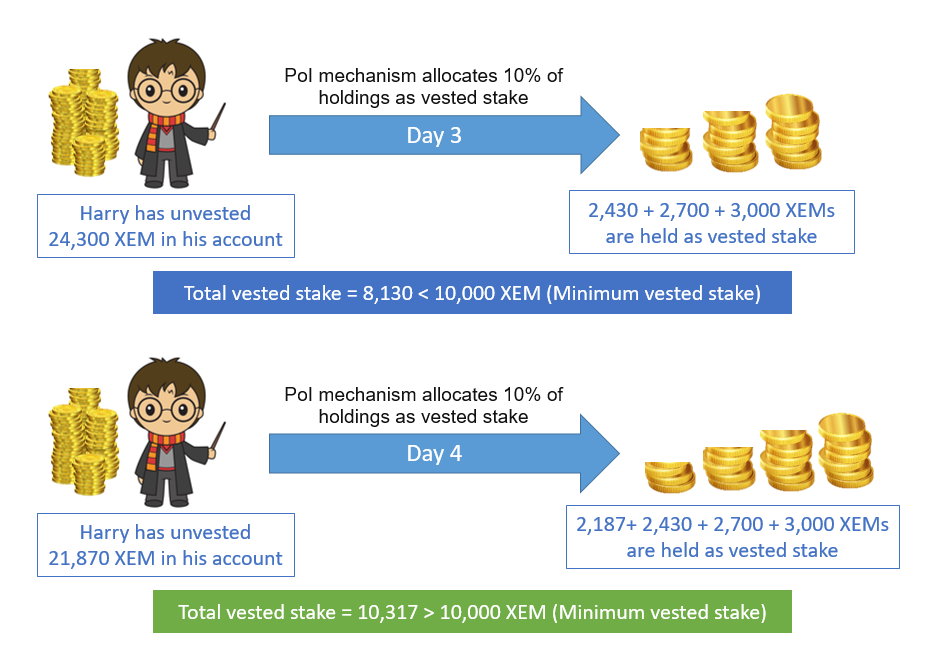
**How does the Proof-of-Importance (PoI) Algorithm work?**

Let’s take an example to understand the Proof of Importance(PoI) mechanism on the NEM Blockchain network.

Harry Potter is a reputed coin hoarder with 30,000 XEMs in his account. He wishes to become a block harvester. So, what could he do to ensure his selection?

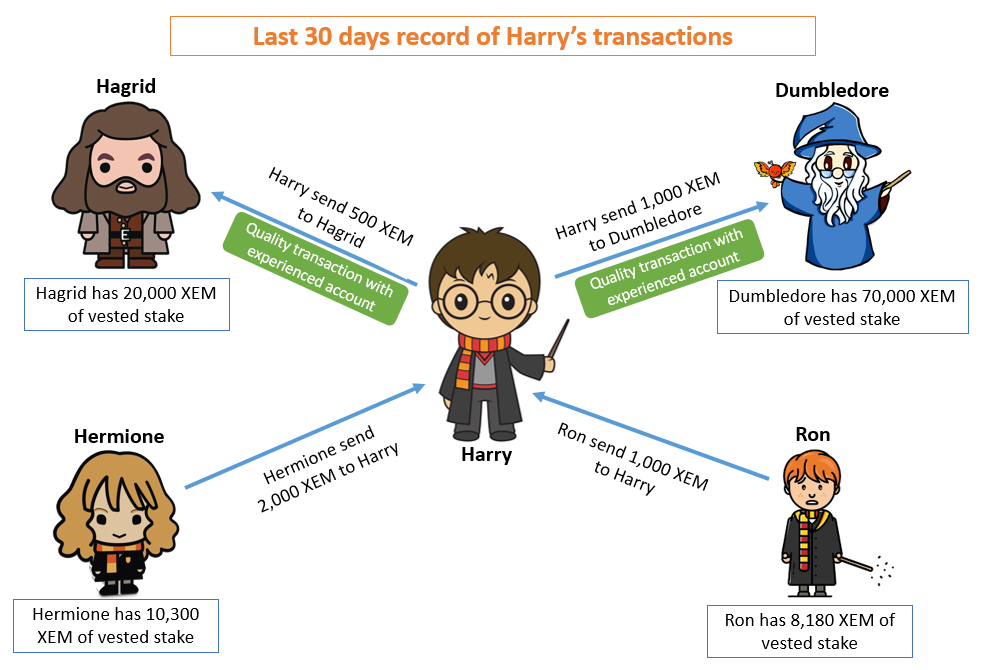
**Target 1: Reach to at least minimum vested stake. (at least 10,000 XEM in this case)**





On day 4 Harry will cross the threshold of minimum vested coins stake. Hence, target one is achieved.

**Target 2: Make regular transactions to quality accounts (with more than 10,000 XEM at vested stake)**



Harry’s account made more than 1000 XEM of transactions in the last 30 days to the quality accounts (having more than 10,000 XEM at a vested stake).

Now, Harry is eligible to become one of the block harvesters in the network.

**Benefits of Proof of Importance (PoI)**

**PoI removes this possibility of Sybil attacks in the following ways**:

1. **By stopping an account staking all 10,000 XEM at once**. 10% of your non-staked XEM becomes staked after every 24 hours. It means an account needs to hold way more than 10K XEM in an account.
2. Another is **using the net loss of the account to help measure the importance score**. Basically, if an account sends XEM and receives it back, it’ll lower its importance score

**X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-X-**