Proof of Importance -

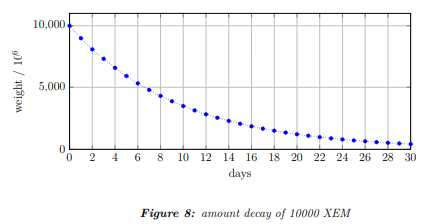
Η απόδειξη της Σημασίας

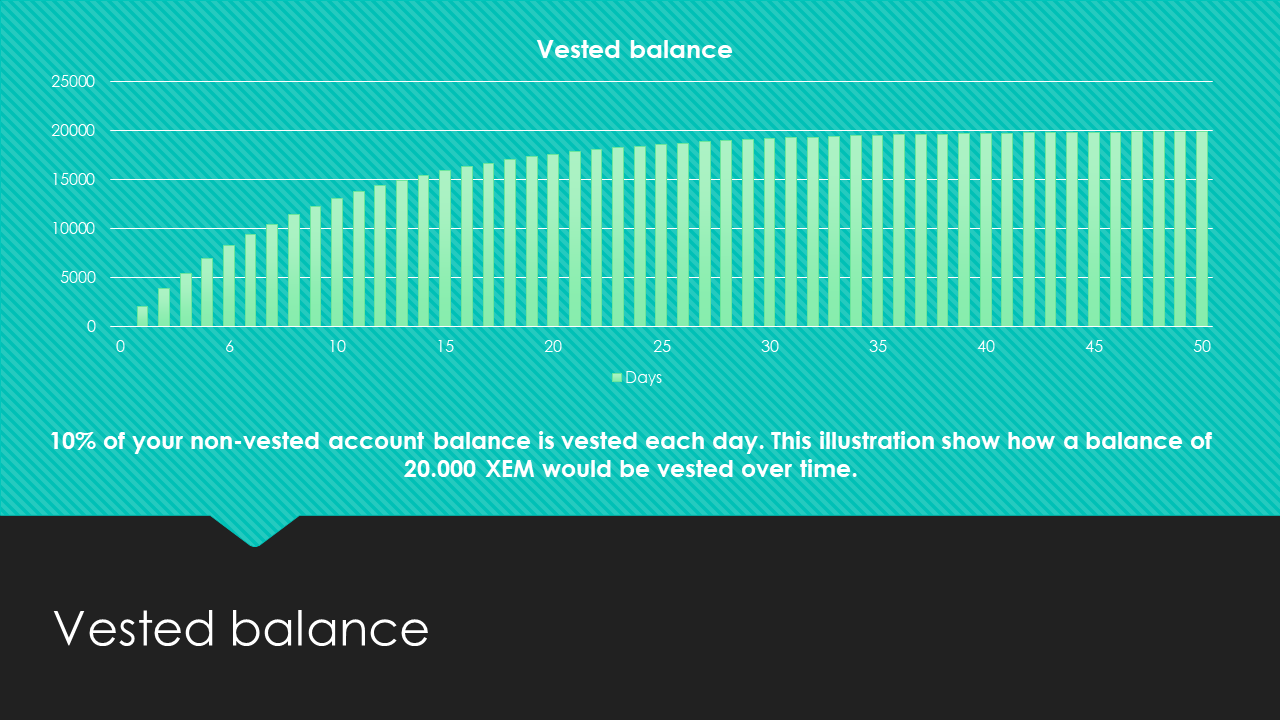
## Mιχούλης Γεώργιος dai16067 dai16067@uom.edu.gr



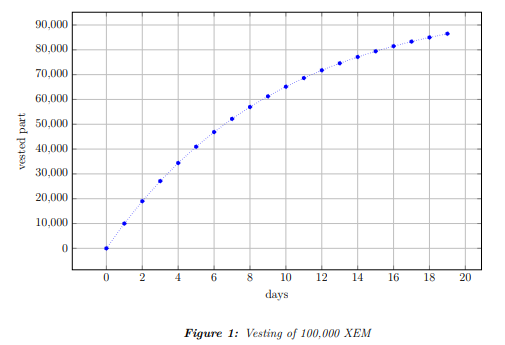


1. Τι είναι το ΡοΙ

H απόδειξη σημασίας ή σπουδαιότητας (PoI – Proof of Importance) είναι o αλγόριθμος συναίνεσης της τεχνολογίας blockchain που χρησιμοποιείται από την εταιρία NEM. Σε αυτό το μοντέλο ο κάθε λογαριασμός έχει μια βαθμολογία σημασίας που αντιπροσωπεύει τη συνολική σημασία που έχει για την οικονομία της NEM. Λογαριασμοί με υψηλότερη βαθμολογικά σημασία έχουν υψηλότερες πιθανότητες για να συλλέξουν (harvest) ένα μπλοκ δηλαδή να εκδώσουν ένα νέο μπλοκ. Επειδή όλες οι συναλλαγές της ΝΕM είναι δημόσιες, το γράφημα συναλλαγής της οικονομίας της μπορεί να υπολογιστεί με ακρίβεια. Άρα η βασική καινοτομία της Απόδειξης Σημασίας είναι ότι ότι το γράφημα των συναλλαγών μπορεί να χρησιμοποιηθεί για την καταγραφή των και την αποσαφήνιση των εισροών για έναν οποιοδήποτε λογαριασμό. Επειδή σε αυτό το δίκτυο υπάρχει μεγάλη διαφάνεια, οι πληροφορίες αυτές με τις μεταφορές μεταξύ των λογαριασμών μπορούν να χρησιμοποιηθούν για την βαθμολόγηση της σπουδαιότητας των λογαριασμών . Τέλος ο πίνακας outlink που ορίζει το γράφημα των συναλλαγών είναι σημαντικός και χρησιμοποιείται στον υπολογισμό του PoI. O πίνακας outlink ουσιαστικά περιγράφει την σταθμισμένη καθαρή ροή ενός λογαριασμούς τις τελευταίες 30 ημέρες, αρά μόνο οι καθαρές μεταφορές συμβάλουν στην σημασία του λογαριασμού αυτού.[1]

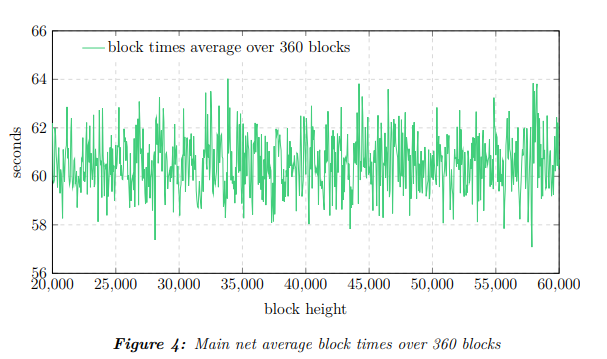
Η απόδειξη της σπουδαιότητας (PoI της ΝΕΜ , χρησιμοποιεί επίσης ένα κρυπτονόμισμα που ονομάζεται XEM. Κάθε λογαριασμός στο δίκτυο NEM έχει ένα υπόλοιπο XEM που χωρίζεται σε δύο μέρη: κατοχυρωμένο και μη επενδυμένο. Κάθε φορά που ένας λογαριασμός λαμβάνει το XEM, αυτό το νέο XEM προστίθεται στο μη επενδυμένο υπόλοιπο του λογαριασμού. Επίσης Το ένα δέκατο του μη επενδυμένου ποσού του κάθε λογαριασμού μεταφέρεται στο κεκτημένο μέρος σε κάθε 1440 μπλοκ (σχεδόν κάθε μέρα). Για να είναι ένας λογαριασμός τόσο “σημαντικός” που να μπορεί να δημοσιεύει καινούργια μπλοκ πρέπει να κατέχει τουλάχιστον 10.000 κατοχυρωμένα XEM, επίσης πρέπει να έχει έναν αξιοσημείωτο βαθμό λογαριασμού εντός του δικτύου (υπολογίζεται με βάση τον αλγόριθμο NCDawareRank),έναν συντελεστή στάθμισης που βασίζεται στην τυπολογική θέση του λογαριασμού (όπως, ο λογαριασμός είναι μια απόκλιση ή μέρος ενός συνόλου κόμβων) και δύο κατάλληλες σταθερές που καθορίζονται από την εταιρία.[4] 

1. Παράδειγμα χρήσης του και πως λειτουργεί το ΡοΙ

Αναφορικά παραθέτω τα βήματα κατά τα οποία μπορεί κάποιον να συμμετέχει στο ΡοΙ της ΝΕΜ. Έστω ότι ένας καινούργιος χρήστης προσπαθεί να εγγραφεί στο δίκτυο της εταιρίας ΝΕΜ. Αρχικά δημιουργείτε ο λογαριασμός του χρήστη με την χρήση ελλειπτικών καμπυλών έτσι ώστε να επιτευχθεί η εξασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και η μη αναίρεσης όλων των συναλλαγών. Κάθε λογαριασμός έχει ένα ιδιωτικό και δημόσιο κλειδί της τάξεως των 256 bit έκαστος με τη χρήση αλγορίθμου Ed25519 . Οι χρήστες και οι λογαριασμοί τους ξεχωρίζουν με τις διευθύνσεις, οι οποίες προέρχονται την μονόδρομη συνάρτηση του Ed25519 των δημόσιων κλειδιών τους. Κάθε λογαριασμός περιέχει: ένα υπόλοιπο λογαριασμό, τον αριθμό των συλλεγμένων μπλοκ, το ύψος της πρώτης συναλλαγής, λίστα με άλλους λογαριασμούς, πληροφορίες σχετικά με την κατάσταση εξουσιοδοτημένου λογαριασμού, βαθμό σημαντικότητας και ΝCD επίπεδο και το κατοχυρωμένο υπόλοιπο. Στη συνέχεια το δημόσιο κλειδί περνά από μια σειρά , 6 βημάτων, από κρυπτογραφικές συναρτήσεις (Ripemd, SHA3) και δημιουργείτε έτσι η διεύθυνση του λογαριασμού αυτού. Με το ιδιωτικό κλειδί δημιουργείται μια ψηφιακή υπογραφή και η ανταλλαγή μηνυμάτων γίνεται με την χρήση του ΑΕS συστήματος.[1]

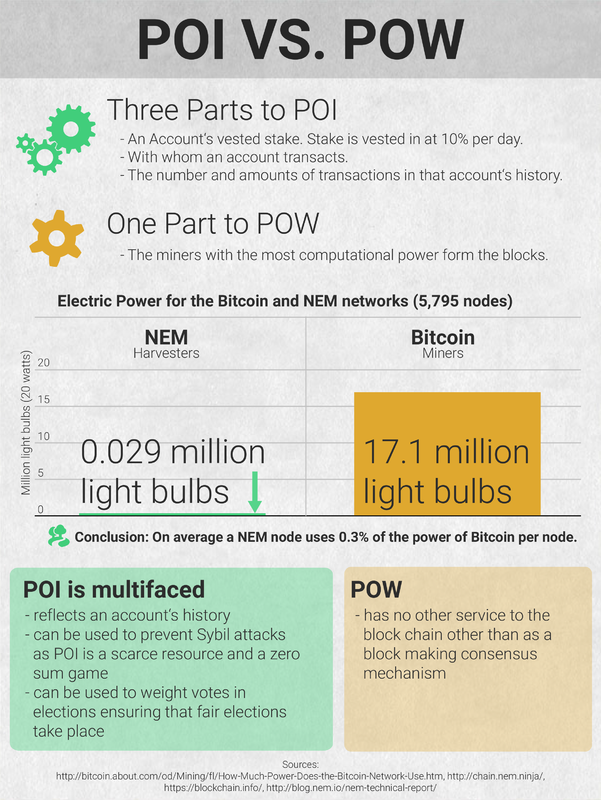
Στην συναλλαγή τώρα ανταλλάσσονται ΧΕΜ κρυπτονομίσματα από τον έναν λογαριασμό στον άλλον. Για κάθε 10.000 ΧΕΜ που ανταλλάσσονται υπάρχει φόρος της τάξεων των 0.5 ΧΕΜ (όριο τα 2.5) και για κάθε 32 bytes μηνύματος που ενθυλακώνεται στην συναλλαγή υπάρχει πάλι 0.5 ΧΕΜ φόρος. Η NEM επιτρέπει την εξουσιοδοτημένη συλλογή – «συγκομιδή» των μπλοκ μέσω της χρήσης ενός άλλου λογαριασμού. Αυτό επιτρέπει στον αρχικό λογαριασμό να χρησιμοποιήσει τη σημασία του για τη συγκομιδή σε έναν απομακρυσμένο διακομιστή χωρίς να χρειάζεται να εκθέσει ανοικτά το ιδιωτικό κλειδί του στο διακομιστή και έτσι δεν εκτίθενται τα κεφάλαια του. Επειδή η ΝΕΜ δίνει αυτό το δικαίωμα έστω ότι ένας λογαριασμός Μ έχει υπόλοιπο 1000 ΧΕΜ σε 3 υπό -λογαριασμούς του, Α, Β και Γ · 100 ΧΕΜ πρέπει να μεταφερθούν από το Μ στο Χ. Αρχικά έστω ότι στέλνονται από το Β όπου αυτό δημιουργεί μια κανονική συναλλαγή των 100 ΧΕΜ με την multisig σφραγίδα των λογαριασμών. Έπειτα το Β ενθυλακώνει την κανονική συναλλαγή και την υπογράφει με την μοναδική υπογραφή τους και τη στέλνει στο δίκτυο, από εκεί το Α και Γ ειδοποιούνται για την αλλαγή και δημιουργούν μια multisig συναλλαγή με το να υπογράψουν την σύνοψη της πρώτης συναλλαγής και την στέλνουν στο δίκτυο. Τέλος αφού όλοι οι λογαριασμού το υπογράψουν τότε η συναλλαγή γίνεται δεκτή από το δίκτυο και γίνεται η μεταφορά. [1]

Στο κομμάτι του blockchain , κάθε μπλοκ έχει τα ίδια περιεχόμενα όπως και με του bitcoin συν την αρχική σύνοψη της αλυσίδας τα οποία κωδικοποιούνται με SHA3 256-bit. Η δυσκολία σύμφωνα με μελέτες λένε ότι ο αλγόριθμος παράγει μπλοκ με μέσο χρόνο 60 ± 0,5 δευτερόλεπτα. Κάθε μπλοκ έχει ένα σκορ που προκύπτει από την διαφορά της δυσκολίας με τον χρόνο που πέρασε από την έκδοση του τελευταίου μπλοκ. Η διαδικασία δημιουργίας νέων μπλοκ ονομάζεται συγκομιδή . Για να δημιουργήσει κάποιος ένα νέο μπλοκ πρέπει να έχει πάνω από 10.000 ΧΕΜ. Ο λογαριασμός μπορεί να δημιουργήσει νέο μπλοκ κάθε φορά που το hit είναι μικρότερο από το target που είναι μια σειρά από μεταβλητές ( διάφορες συναρτήσεις διασποράς, λεπτά , σημαντικότητα των λογαριασμών του, δυσκολία νέου μπλοκ). Με αυτό το τρόπο λοιπόν δημοσιεύονται καινούργια μπλοκ στο δίκτυο. Ο συγχρονισμός της αλυσίδας ελέγχεται από έναν αλγόριθμο της ΝΕΜ και αντιμετωπίζει τις διάφορες διακλαδώσεις (forks). [1]



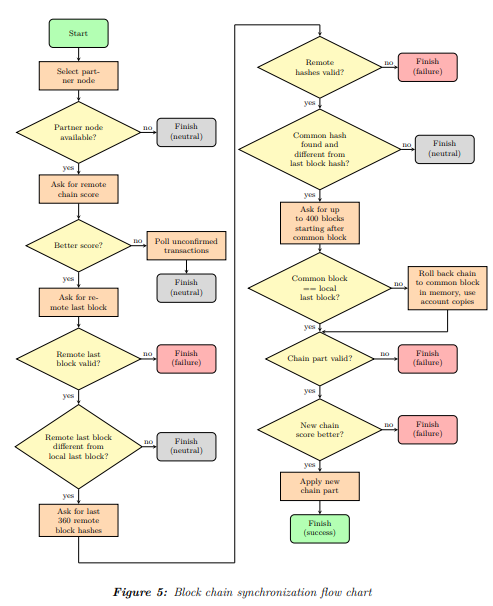
1. Σύγκριση με ΡοW

Το PoI μοιάζει περισσότερο με το ΡοS πάρα με το PoW. Γενικά γνωρίζουμε ότι το PoW είναι αρκετά χρονοβόρο στην έκδοση νέων μπλοκ και χρειάζεται πολύ ενέργεια για να λειτουργεί. Το PoI χρησιμοποιεί πολύ μικρή ενέργεια κάτι που είναι αρκετά οικολογικό και οικονομικό και εκδίδει νέα μπλοκ σε πολύ μικρό χρονικό διάστημα. To PoI είναι ένα δημόσιο δίκτυο που αντέχει σε κακόβουλες επιθέσεις, βασίζεται στις συναλλαγές και στους λογαριασμούς του, χρησιμοποιεί την Golang, C++, Solidity, Serpent, LLL, τρέχει και σε VM και τοπικά αφορά γενικές χρήσεις και το πιο γνωστό είναι το Βitcoin. Από την άλλη το PoI είναι ένα δημόσιο αλλά και ιδιωτικό δίκτυο , δεν γνωρίζουμε ακόμα πόσο αντέχει σε επιθέσεις, βασίζεται και αυτό στους λογαριασμούς και στις συναλλαγές, χρησιμοποιεί μόνο java, είναι μια πλατφόρμα blockchain και το πιο γνωστό και μοναδικό κρυπτονόμισμα είναι το XEM. Επίσης παρόλο που η ΝΕΜ έχει πάρει κάποια μετρά εναντίον των Sybil Attack ,loop attack και Nothing at-stake,[1] στο PoW είναι τέτοια η δομή του για να τα αποτρέπει πριν καν ανιχνευθούν, άρα σε αυτές τις περιπτώσεις το PoW είναι πιο ασφαλές. [2]

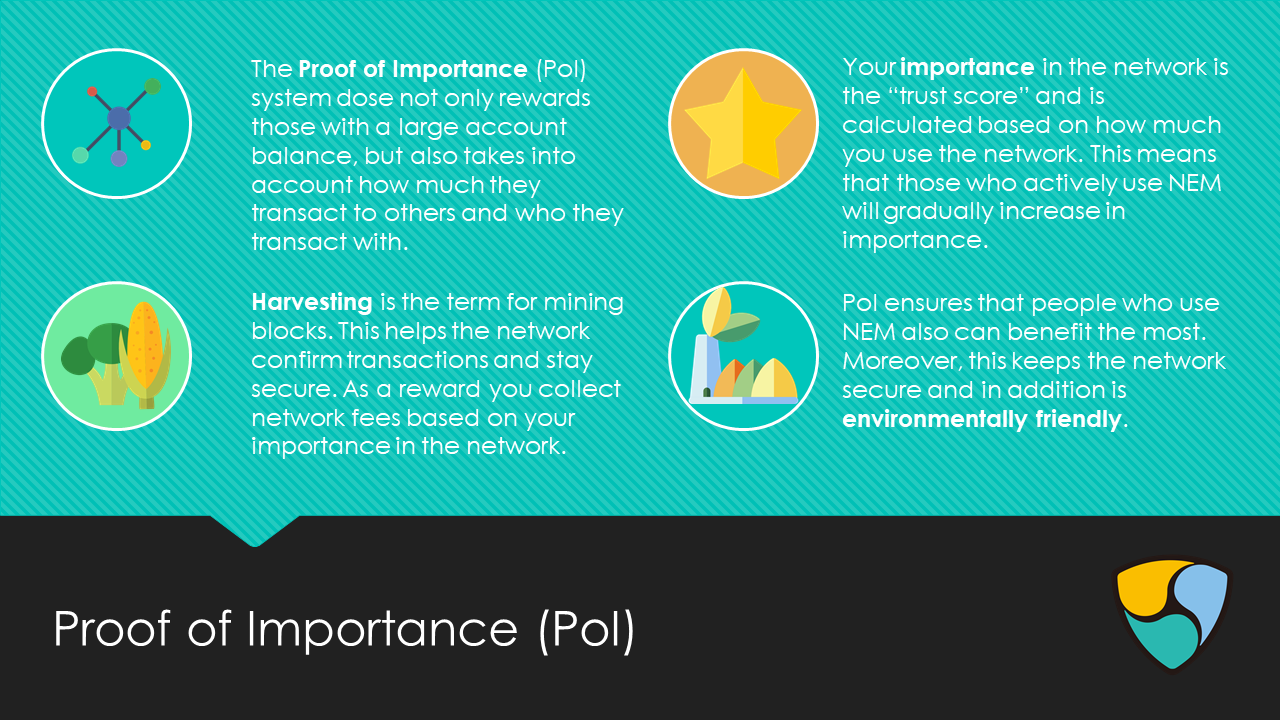


4. Θετικά και αρνητικά

Το PoI σε γενικές γραμμές είναι αρκετά καλό. Πέρα από την ταχύτητα και την εξοικονόμηση ενέργειας που προσφέρει, έχει την πολυτέλεια ότι οι πλούσιοι δεν μπορούν να γίνονται συνέχεια πλουσιότεροι ( όπως το PoS) στην πλατφόρμα επειδή το ποσό των μετρητών που έχει ένας λογαριασμός δεν είναι ο μόνος παράγοντας που λαμβάνεται υπόψη κατά τη ιεράρχηση της φήμης-σημαντικότητας ενός λογαριασμού. Ενώ αντίθετα το πρόβλημα που υπάρχει σε πολλές πλατφόρμες ( και στο PoS) δηλαδή, της χρήσης εικονικών-ψεύτικων συναλλαγών που οφείλει τους επιτήδειους στην αποστολή μπροστά και πίσω των συναλλαγών ώστε να εξαπατήσουν τον αλγόριθμο της εκάστοτε εταιρίας, είναι ένα μείζον ζήτημα που η ΝΕΜ ακόμα δεν έχει λύσει. [3]



1. Συμπέρασμα

Τελικά ο αλγόριθμος εξαρτάται από το πόσο ενεργός είναι κάποιος στο δίκτυο. Όσο πιο ενεργός είναι κάποιος τόσες περισσότερες ανταμοιβές θα λαμβάνει. Η υψηλότερη φήμη φέρνει και περισσότερες ανταμοιβές. Ουσιαστικά ο αλγόριθμος ευνοεί τις δραστηριότητες του κάθε χρήστη και όχι τόσο από τις συναλλαγές που έχει πραγματοποιήσει. Πολύ σημαντικό είναι ότι η φήμη του δεν εξαρτάται από το λεγόμενο “stake” αλλά είναι ένα μέρος ενός μεγαλύτερου συνόλου. Οπότε το σύστημα ψηφοφορίας ( το οποίο αφορά την εξέλιξη της πλατφόρμας γενικότερα) είναι πιο δημοκρατικό σε σχέση με αυτό του ΡοS [5].

Εν κατακλείδι μπορούμε να πούμε ότι, το ΡοΙ είναι μια τεχνολογία που ακόμα βρίσκεται υπό ανάπτυξη αλλά έχει πολλές δυνατότητες να εξελιχθεί σε κάτι πολύ μεγάλο. Το ότι είναι αρκετά οικολογικό είναι ο πιο καταληκτικός παράγοντας για την ανάπτυξη του και θα μπορέσει να ανταγωνιστεί επάξια τους ανταγωνιστές του. Το ότι χρησιμοποιεί σε κάθε στάδιο συναλλαγής πολλές διαφορετικές κρυπτογραφικές συναρτήσεις το κάνει αρκετά ασφαλής στην χρήση του, όπως στην δημιουργία λογαριασμού που έχουμε τις ελλειπτικές καμπύλες, αλλά και στην δημιουργία διεύθυνσης που έχουμε την χρήση του SHA3 και του Ripemd. Ακόμα το τέλειο μοντέλο συναίνεσης δεν υπάρχει οπότε είναι μεγάλος ακόμα ο δρόμος μπροστά.

1. Βιβλιογραφία

[1] Νem.io. (2018). *ΝΕΜ Technical Reference*. [online] Available at: <https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf>.

[2] N. Chalaemwongwan and W. Kurutach, "State of the art and challenges facing consensus protocols on blockchain," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018.  
[online] Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8343266&isnumber=8343066>

[3] Medium. (2019). *Blockchain Basics — PoW vs. Pos vs. PoI*. [online] Available at: <https://medium.com/the-mission/blockchain-basics-pow-vs-pos-vs-poi-48d04928c7d6>.

[4] L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018,   
[online] Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8400278&isnumber=8399814>

[5] NEM News Website. (2017). *Releasing the NEM Voting Module - NEM News Website*. [online] Available at: <https://nemflash.io/releasing-nem-voting-module/>.

Σχόλια: το importance άλλοτε το μεταφράζω σημασία ή σπουδαιότητα ή φήμη λόγο κακής μετάφρασης και αγγλικών μου. Επίσης το harvesting άλλοτε συγκομιδή άλλοτε συλλογή.