



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΩΣ
UNIVERSITY OF PIRAEUS

Σχολή Τεχνολογίων Πληροφορικής
και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Ερευνητική Εργασία στο Μάθημα «Ασφάλεια Δικτύων»

Υλοποίηση συστήματος Αποκεντρωμένων Εκλογών στο Blockchain του Ethereum



Καθηγητής: **Χρήστος Ξενάκης**

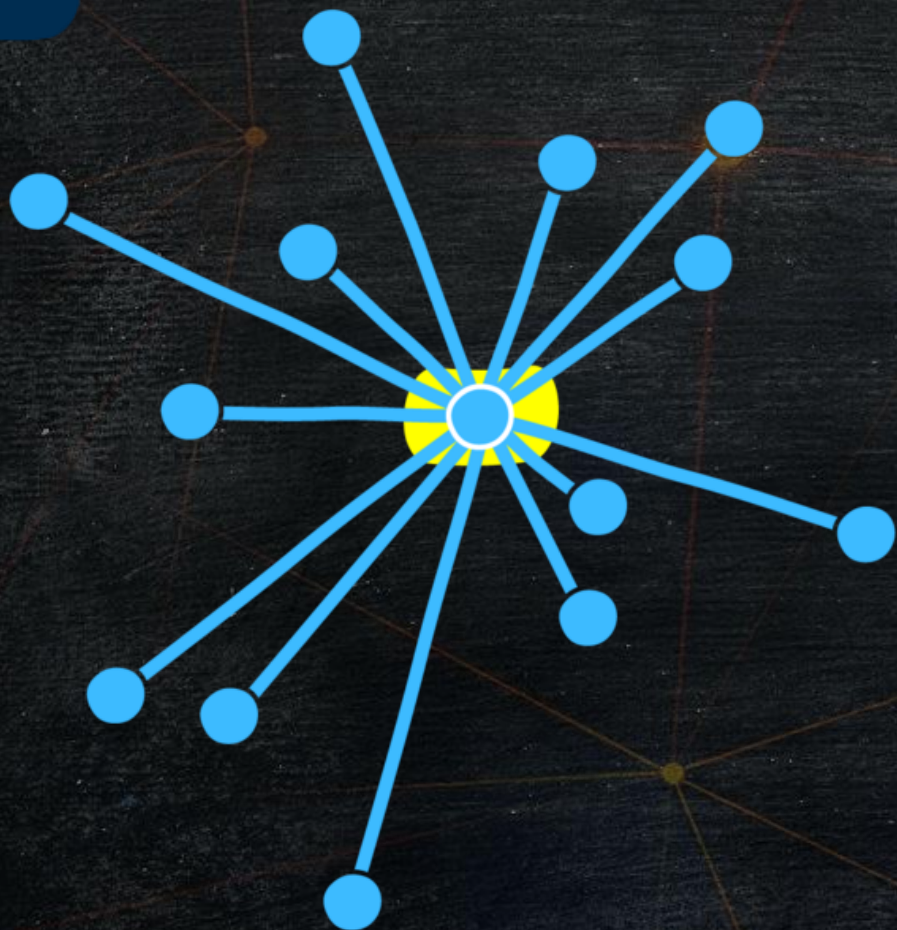
Όνοματα φοιτητών : **Δημήτριος Βαγιακάκος, Σταύρος Γκίνος, Κωνσταντίνος Καραχάλης**
E18019 E18043 E18065

Πειραιάς, Ιανουάριος 2021

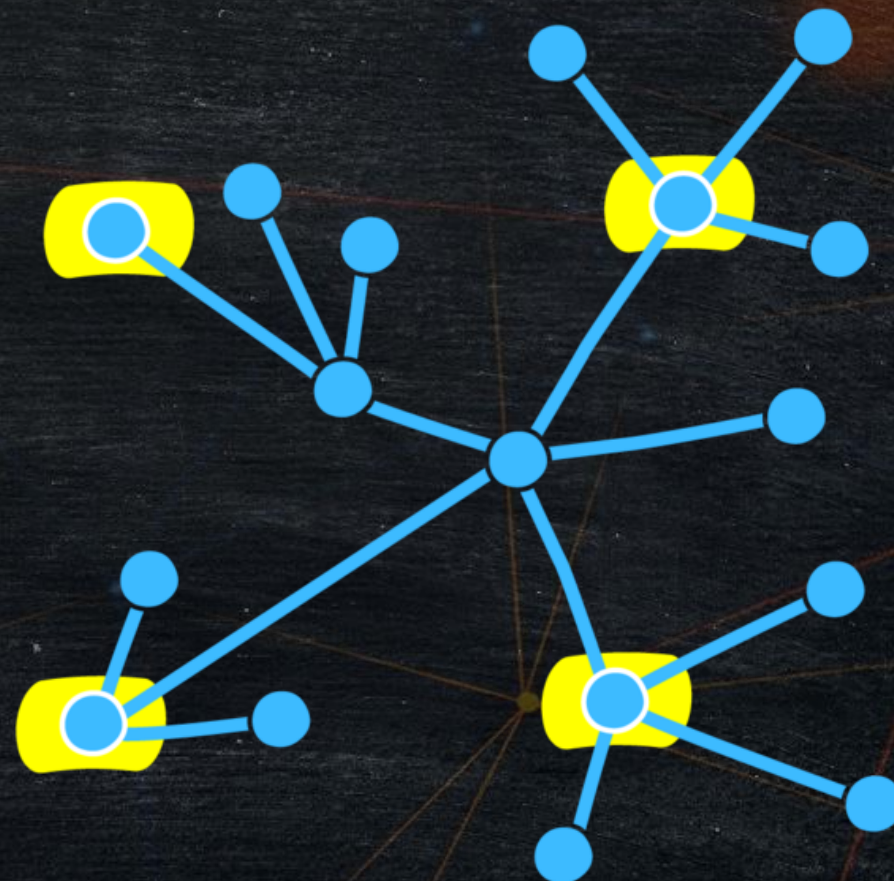


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΩΣ
UNIVERSITY OF PIRAEUS

Σχολή Τεχνολογιών Πληροφορικής
και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων



Κεντροποιημένο Δίκτυο



Αποκεντροποιημένο Δίκτυο



Το Blockchain είναι μία peer-to-peer τεχνολογία όπου κρατάει μητρώο συναλλαγών, χωρίς κάποιον υπεύθυνο να το ελέγχει, έτσι ώστε όλες οι συναλλαγές-πληροφορίες να είναι διαθέσιμες σε όλους τους χρήστες πάνω στο ίδιο δίκτυο.

Το Blockchain αποτελεί μία επαναστατική τεχνολογία, αφού δίνει την δυνατότητα να στηθούν αποκεντρωμένες υπηρεσίες, πράγμα που καθιστά το δίκτυο αξιόπιστο από ενδεχόμενες τροποποιήσεις τρίτων όπου θα μπορούσαν να συμβούν στα παραδοσιακά κεντροποιημένα δίκτυα (π.χ νοθεία εκλογών) .

Οι περισσότεροι, ήρθαμε για πρώτη φορά σε επαφή με το Blockchain, μέσω του Κρυπτονομίσματος **Bitcoin**  , το οποίο πρόσφατα έσπασε και νέο ρεκόρ αξίας. Ωστόσο, το Blockchain είναι κάτι πολύ περισσότερο από τα κρυπτονομίσματα. Οι εφαρμογές όπου θα μπορέσει να έχει το Blockchain στην καθημερινή μας ζωή είναι πολλές, όπως είναι η παροχή πιο αξιόπιστων τραπεζικών συναλλαγών, παροχή διάφορων υπηρεσιών στους κλάδους της υγείας, των έξυπνων πόλεων, αλυσίδες εφοδιασμού, πολιτικά και γεωπολιτικά ζητήματα κ.α.



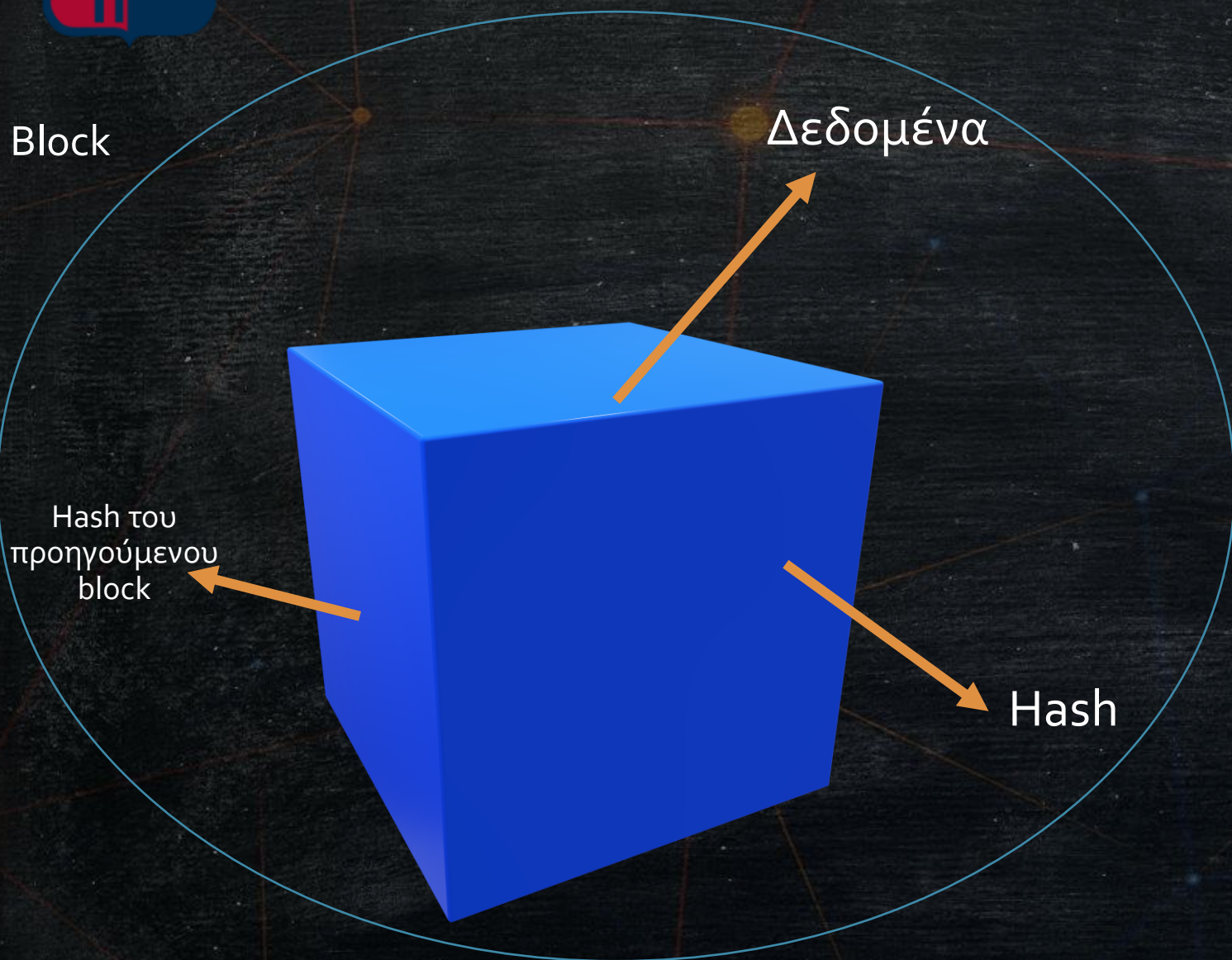
Κύρια χαρακτηριστικά του Blockchain:

1. Δεν μπορεί να γίνει corrupt.

Κάθε node του δικτύου έχει ένα αντίγραφο του blockchain. Για να προστεθεί ένα block, πρέπει να ελέγχεται για την εγκυρότητά του.

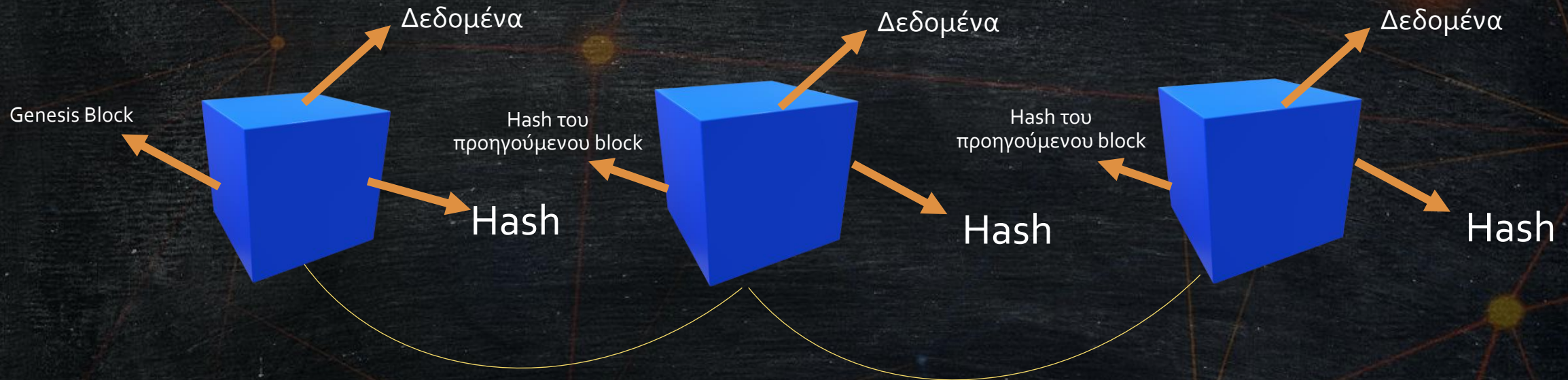


2. Αποκεντρωμένο και με ενισχυμένη Ασφάλεια.
Το δίκτυο είναι αποκεντρωμένο, που σημαίνει ότι κανείς τρίτος ή κάποια κυβέρνηση δεν μπορεί να το ελέγξει ή να το τροποποιήσει.



Κάθε block, αποτελείται από δεδομένα, το Hash του και το Hash του προηγούμενου block. Μόλις δημιουργηθεί το block, υπολογίζεται το hash, το οποίο είναι μονόδρομο (Μήνυμα \rightarrow Hash, Hash \nrightarrow Μήνυμα).

Αυτό σημαίνει, ότι οποιαδήποτε αλλαγή πάνω στο block, αλλάζει εντελώς το hash, άρα δεν είναι το ίδιο block.



Hash: 1X4R	Hash: 43U8	Hash : 43JM8
Previous hash: 0000	Previous hash: 1X4R	Previous hash: 43U8

Και έτσι φτιάχνεται μία αλυσίδα απο blocks. Το πρώτο block, από αυτό δηλαδή που ξεκινάει το blockchain, ονομάζεται Genesis Block.

Ωστόσο, εδώ θα μπορούσε να επισημανθεί ότι, στις ημέρες μας, υπάρχει αρκετά μεγάλη υπολογιστική ισχύ, έτσι ώστε να είναι δυνατόν να ξαναυπολογιστούν ξανά όλα τα hash των υπολοίπων block. Έτσι, χρησιμοποιείται ένας επιπλέον μηχανισμός ασφαλείας.



Οι 2 πιο γνωστοί Αλγόριθμοι που λειτουργούν τα Blockchain

Proof Of Work:

Το block προσπαθεί να μας αποδείξει ότι όντως δούλεψε.

Για να προστεθεί ένα block στην αλυσίδα, οι miners πρέπει να λύσουν επιτυχώς ένα «puzzle», χρησιμοποιώντας την υπολογιστική τους ισχύ.

Έτσι, για να καταφέρει κάποιος να επηρεάσει το αποτέλεσμα, πρέπει να ελέγχει πάνω από το 51% του δικτύου.

Ο πρώτος miner που θα επιλύσει το puzzle, ανταμείβεται για την δουλειά του.

Όπως είναι κατανοητό, όσο περνάει ο καιρός, τόσο πιο δαπάνηρη γίνεται η διαδικασία, κάνοντας εξαιρετικά δύσκολο το Mining αν δεν έχεις αρκετή υπολογιστική ισχύ,

Χαρακτηριστικό που αποτελεί και μειονέκτημα, μιας και σπαταλούνται εκατομμύρια κιλοβατώρες κάθε χρόνο.

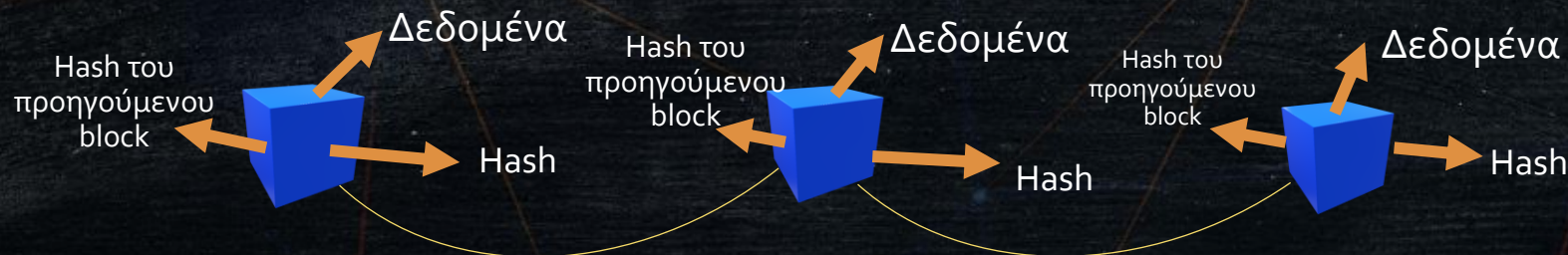
Proof Of Stake:

Στο Proof Of Stake, δεν υπάρχει διαγωνισμός στο ποιός θα επιλύσει το puzzle πρώτος, μιας και ο αλγόριθμος βασίζεται στο stake. Δηλαδή, ο αλγόριθμος επιλέγει ψευδοτυχαία έναν validator. Μόλις επιλεγεί ένας Validator, έχει το αποκλειστικό δικαίωμα να φτιάξει block.

Έτσι, οι υπόλοιποι Validators δεν σπαταλούν ενέργεια να κάνουν την οποιαδήποτε πράξη μιας και δεν επιλέχθηκαν. Επιπλέον, αν ο Validator προσπαθήσει να κάνει κάτι ακατάλληλο, τότε θα χάσει το stake του.


Έτσι, για να καταφέρει κάποιος να επηρεάσει το αποτέλεσμα, πρέπει να έχει την κατοχή του το 51% του κρυπτονομίσματος του δικτύου. Κάτι που είναι εξαιρετικά δύσκολο να συμβεί.

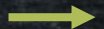

Το Power Of Work χρησιμοποιείται στο Bitcoin , και σε άλλα διάσημα blockchain. Το Ethereum  χρησιμοποιεί μία δική του έκδοση του Power Of Work (Ethash), μέχρι που θα περάσει σε Power Of Stake.







Ethereum:

Το Ethereum  είναι ένα ανοικτού κώδικα (open-source) Blockchain, το οποίο αποτελεί μία αποκεντρωμένη δομή, η οποία, εκτός από το γνωστό κρυπτονόμισμα της, το Ether, μπορεί να εκτελέσει αποκεντρωμένα προγράμματα, τα οποία ονομάζονται Smart Contracts.

Το σημαντικότερο χαρακτηριστικό των Smart Contracts  Ότι είναι αμετάβλητα! Από την στιγμή που θα γίνουν deployed, ο κώδικας τους δεν μπορεί να τροποποιηθεί ή να αλλάξει. Τα Smart Contracts γράφονται στην γλώσσα προγραμματισμού Solidity , η οποία έχει σχεδιαστεί για να τρέχει στο EVM (Ethereum Virtual Machine).




Ο μόνος τρόπος για να αλλάξει ή να τροποποιηθεί ο κώδικας, είναι να γίνει ξανά deploy το smart contract με τις νέες αλλαγές. Επιπλέον, τα αποτελέσματα του smart contract, είναι ίδια για όλους τους χρήστες όπου το εκτελούν.

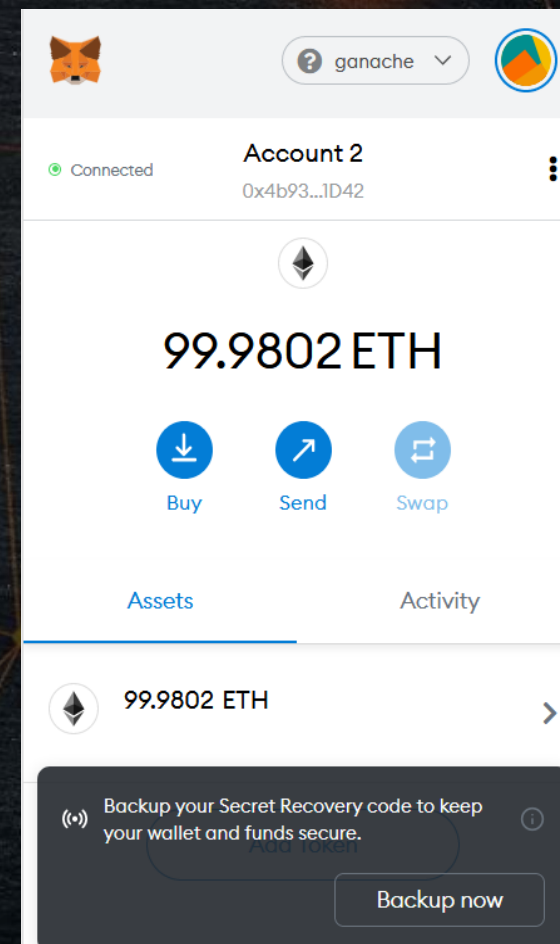
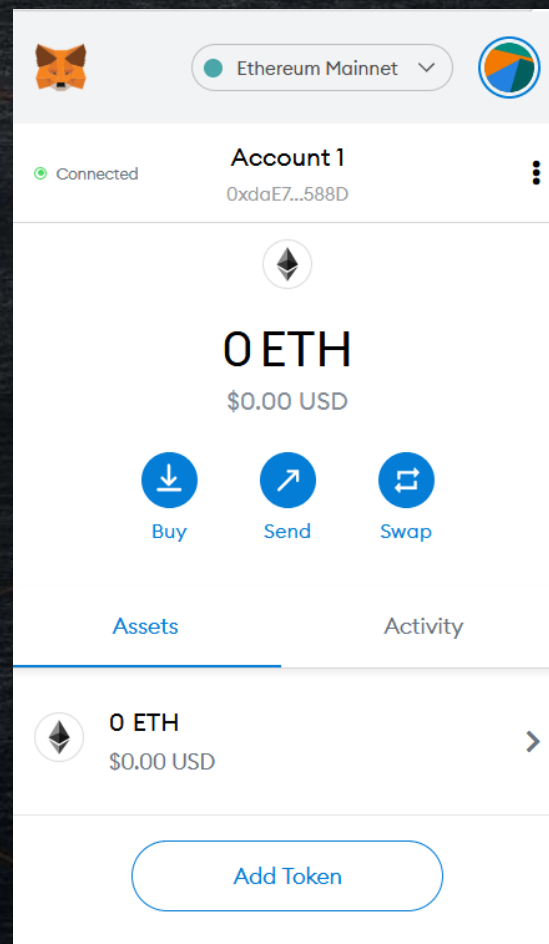
Για να έρθουμε σε επαφή με ένα Smart Contract μέσω του browser μας, χρησιμοποιούμε τις βιβλιοθήκες της Web3.js όπου είναι ένα JavaScript  API για να συνδεθούμε στο δίκτυο του Ethereum . Το Web3 είναι μία αναβάθμιση του Web2 όπου εστιάζει σε ένα αποκεντρωμένο διαδίκτυο, με αποκεντρωμένες εφαρμογές που κανείς δεν μπορεί να ελέγχει.





Το Ψηφιακό μας πορτοφόλι:

Το Metamask  αποτελεί μια εφαρμογή που χρησιμοποιείται ως ψηφιακό πορτοφόλι για το Ethereum  πραγματοποιώντας συναλλαγές με ether, που αποτελούν το κρυπτονομίσμα του Ethereum , και εγκαθίσταται ως επέκταση των προγραμμάτων περιήγησης όπως το Mozilla Firefox, Google Chrome κλπ. Χαρακτηριστικό του είναι ότι μπορεί να χρησιμοποιηθεί για να συνδεθούμε και σε local blockchain, εκτός από το main Ethereum Blockchain.





ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΩΣ UNIVERSITY OF PIRAEUS

Στα πλαίσια της εργασίας μας, υλοποιήσουμε ένα σύστημα αποκεντρωμένων εκλογών στο Blockchain του Ethereum.

Η εργασία υλοποιήθηκε στην έκδοση 0.8.0 της Solidity.

Κάθε διεύθυνση του Blockchain έχει δικαίωμα να ψηφίσει μόνο μία φορά στις εκλογές.

Το Metamask μας είναι απαραίτητο διότι αποθηκεύει στο Wallet μας την address και το private key, έτσι ώστε να μπορούμε να ψηφίσουμε.

Το Ganache αποτελεί μια εφαρμογή η οποία δημιουργεί ένα τοπικό Blockchain στον υπολογιστή μας, με διάφορα local addresses & τα private keys τους, έτσι ώστε να μπορούμε να δοκιμάζουμε την αποτελεσματικότητα του κώδικα μας άμεσα, κάνοντας τοπικά transactions.

Τέλος, αλληλεπιδρούμε με το local Blockchain μέσω του Web3 από τον Browser (στην διεύθυνση localhost:3000), ο οποίος συνδέεται στο Blockchain, στο οποίο έγινε compile και εκτελείται μέσω του Truffle στον υπολογιστή μας.

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών Τμήμα Ψηφιακών Συστημάτων

Great Ethereum Election

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	0
3	Candidate 3	0
4	Candidate 4	0
5	Candidate 5	0

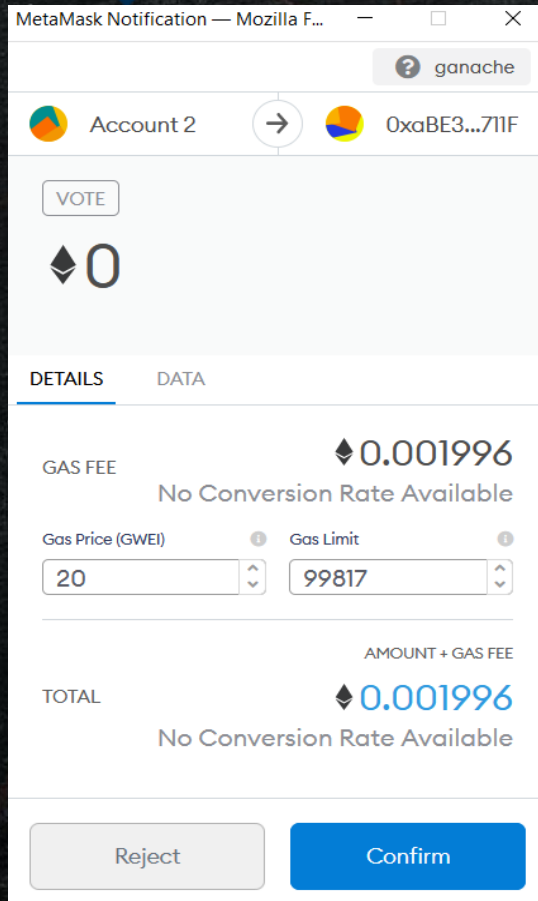
Select Candidate

Candidate 3

Vote

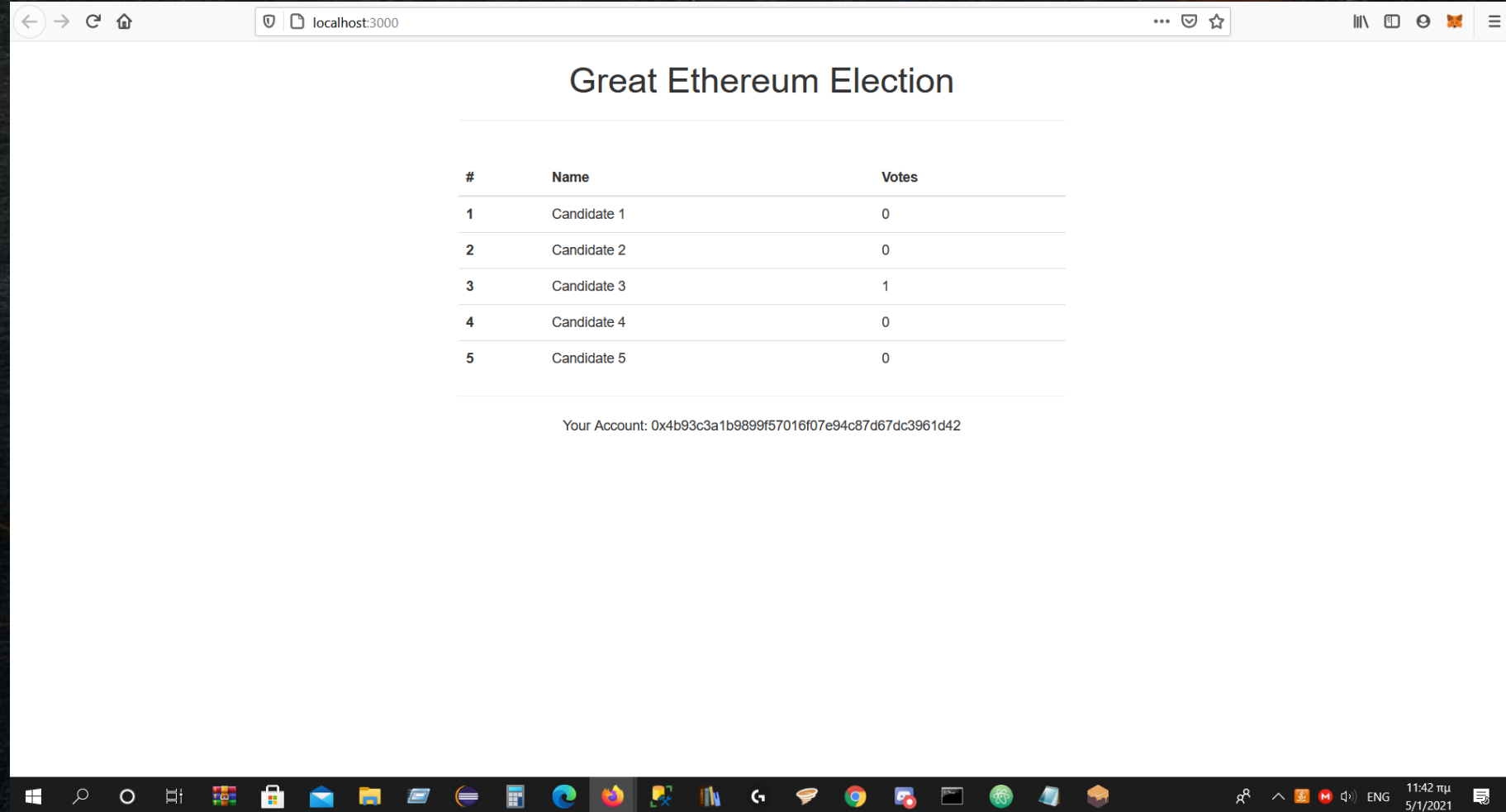
Your Account: 0xdae7ee8dd44a8135bbf04f9413dea50a6aea588d

Στο συγκεκριμένο παράδειγμα, δοκιμάζουμε να ψηφίσουμε τον Candidate 3. Μόλις κάνουμε click στο Vote, θα ανοίξει το ψηφιακό μας πορτοφόλι για την επιβεβαίωση της συναλλαγής (όπου στην προκειμένη περίπτωση είναι η ψήφος μας.)



Screenshot, για την αποδοχή της ψήφου.

Βλέπουμε και το gas όπου θα ξοδευτεί όπου είναι το transaction fee για τον Validator.



Screenshot κατά την ψήφο του 3^{ου} Candidate, βλέπουμε ότι αυξήθηκαν κατά ένα οι συνολικοί ψήφοι.



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΩΣ
UNIVERSITY OF PIRAEUS

Σχολή Τεχνολογίων Πληροφορικής
και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Σας ευχαριστούμε για τον χρόνο σας!

Παρακαλούμε παραθέστε τις απορίες σας!