Co-funded by the
Erasmus+ Programme
of the European Union

A KNOWLEDGE ALLIANCE FOR BLOCKCHAIN IN ACADEMIC, ENTREPRENEURIAL AND INVESTMENT TRAINING

601063-EPP-1-2018-1-CY-EPPKA2-KA

Translated Syllabi-Greek

Deliverable 15
WP5: Content Development Task 5.3

30-10-2020

Table of Contents

Authors and Reviewers

Written by	Organization	Reviewed by	Organization
Dimitris Bibikas	SEERC	Soulla Louca	UNIC
Valentinos Theofilou	UNIC		
Korina Papadopoulou	GNOMON		
	SEERC		

Ενότητα μάθησης 0: Εισαγωγή στο μάθημα και στον κόσμο των DLT

Περιγραφή

Η Ενότητα Μάθησης 0 χωρίζεται σε δύο μέρη.

Το πρώτο μέρος αποτελεί την εισαγωγή στα μαθήματα του DLT4All, προσδιορίζοντας/ξεχωρίζοντας τις κατηγορίες κοινών και κομμάτια από το εκπαιδευτικό υλικό, έτσι ώστε να προσδιοριστεί σε οποίους απευθύνεται το κάθε μάθημα, παρουσιάζοντας μια επισκόπηση για τις διάφορες επιλογές Πιστοποίησης που μπορεί να παρασχεθεί στον μαθητή.

Το Δεύτερο μέρος, περιλαμβάνει την εισαγωγή στις τεχνολογίες του Blockchain, έχοντας ως στόχο την εμπεριστατωμένη τεκμηρίωση τόσο Ιστορικά αλλά και τεχνικά. Ακολούθως, θα αναλυθούν οι βασικές έννοιες και η δομή της τεχνολογίας του Blockchain, οι οποίες θα αναπτυχθούν στα επόμενα μαθήματα.

Στη συνέχεια, θα ακολουθήσει μια διανομή/ταξινόμηση των δικαιωμάτων ανάγνωσής και γραφής του Blockchain, όπως επίσης και οι βασικές έννοιες των Κρυπτονομισμάτων (cryptocurrencies), των Έξυπνα Συμβόλαια (Smart Contracts) και των Αποκεντρωμένων εφαρμογών (Decentralized Applications). Το μάθημα, ολοκληρώνεται με την περιγραφή διαφόρων περιπτώσεων χρήσης της τεχνολογίας (Use cases)

Στόχοι μαθήματος

- Η παρουσίαση της δομής και του περιεχόμενου των μαθήματων του DLT4All
- Ο καθορισμός των διαφορετικών ειδών κοινού των μαθήματων του DLT4All
- Η περιγραφή των διαθέσιμων επιλογών πιστοποίησης για των συμμετεχόντων
- Να δοθεί μια ιστορική επισκόπηση της εξέλιξης της τεχνολογίας Blockchain
- Να δοθεί μια επισκόπηση των τεχνολογικών στοιχείων ενός συστήματος βασισμένου σε Blockchain
- Να παρουσιαστεί ένας χαρακτηρισμός του Blockchain με βάση τα δικαιώματα ανάγνωσης / γραφής του χρήστη
- Η περιγραφή των εννοιών των Κρυπτονομισμάτων (Crypto currencies), των Έξυπνα Συμβόλαια (Smart Contracts) και των Αποκεντρωμένων Εφαρμογών στο πλαίσιο ενός συστήματος που βασίζεται σε Blockchain
- Η παρουσίαση μιας σειράς διαφόρων περιπτώσεων χρήσης της τεχνολογίας (Use Cases) συστημάτων που βασίζονται σε Blockchain

Μαθησιακά αποτελέσματα

- Ανάκληση της δομής του μαθήματος DLT4All
- Επιλογή των κατηγοριών του κοινού στο οποίο στοχεύει το κάθε μάθημα
- Η κατανόηση των διαθέσιμων επιλογών πιστοποίησης
- Η Περιγραφή της ιστορικής εξέλιξης των τεχνολογιών Blockchain
- Η Περιγραφή των τεχνικών στοιχείων ενός συστήματος που βασίζεται σε Blockchain
- Η Περιγραφή της ταξινόμησης των λειτουργιών του Blockchain

- Η κατανόηση της έννοιας των Κρυπτονομισμάτων (Cryptocurrencies), των Έξυπνα Συμβόλαια (Smart Contract) και των Αποκεντρωμένων Εφαρμογών (dApps)
- Η αναγνώριση και περιγραφή διαφόρων περιπτώσεων χρήσης Blockchain (Use Cases)

Περίληψη

1. Εισαγωγή στο DLT4ALL
    1.1. Κατηγοριοποίηση Κοινού
    1.2. Δομή Μαθημάτων
    1.3. Επιλογές Πιστοποίησης
2. Εισαγωγή στο Blockchain
    2.1. Ιστορική Αναδρομή
    2.2. Τεχνολογικά στοιχεία συστημάτων που βασίζονται στο Blockchain
3. Χαρακτηριστικά του Blockchains
    3.1. Δημόσιο (Public) vs Ιδιωτικό (Private) και Χωρίς Άδεια (Permissionless) vs Δανειοδοτημένο (Permissioned)
4. Από το Blockchain στις Αποκεντρωμένες Εφαρμογές (dApps)
    4.1. Κρυπτονομίσματα (Cryptocurrencies)
    4.2. Έξυπνα Συμβόλαια (Smart Contracts)
    4.3. Αποκεντρωμένες Εφαρμογές (Decentralized applications)
5. Περιπτώσεις Χρήσης (Use cases)

Ενότητα Μάθησης 1: Σχεδιασμός P2P βάσεων δεδομένων

Περιγραφή

Η δυνατότητα ανοιχτών, κοινόχρηστων βάσεων δεδομένων με πιστοποιημένα και δημόσια επαληθεύσιμα δεδομένα μπορεί να οδηγήσει σε μεγαλύτερα επίπεδα συμμετοχής και ενδυνάμωσης των πολιτών σε πολλούς τομείς. Η πρώτη ενότητα μάθησης παρέχει μια εις βάθος συζήτηση για θέματα αρχιτεκτονικού σχεδιασμού της P2P διαχείρισης δεδομένων. Οι προκλήσεις που αντιμετωπίζει ο σχεδιασμός μιας κατανεμημένης και αποκεντρωμένης βάσης δεδομένων παρουσιάζονται και αναλύονται σε λεπτομέρεια, εισάγοντας τις βασικές αρχές του σχεδιασμού βάσεων δεδομένων και τους μηχανισμούς στους οποίους βασίζεται ο P2P τρόπος επικοινωνίας. Αναφέρονται δυσκολίες κατά την ανάπτυξη μιας αξιόπιστης βάσης δεδομένων peer-to-peer και παρουσιάζονται πιθανές λύσεις σε προβλήματα που εμφανίζονται σε τεχνολογίες blockchain. Οι συμμετέχοντες στην συγκεκριμένη ενότητα μάθησης θα κατανοήσουν με ποιους τρόπους μπορεί να γίνει κοινή χρήση και συγχρονισμός μιας βάσης δεδομένων μεταξύ διαφορετικών κόμβων και τους λόγους για τους οποίους δεν είναι εύκολο να αλλάξει η δομή της αργότερα. Έτσι θα είναι σε θέση να προσδιορίσουν πότε είναι κατάλληλη η χρήση κατανεμημένης βάσης δεδομένων. Θα καταλάβουν γιατί μια κατανεμημένη βάση δεδομένων είναι αξιόπιστη και πώς αυτή η τεχνολογία μπορεί να κάνει τις συναλλαγές και την κοινή χρήση δεδομένων εντός της αλυσίδας πληροφορίας πιο ασφαλείς. Η ενότητα μάθησης θα αναφερθεί σε στρατηγικές δημιουργίας blockchain ad-hoc βάσεων δεδομένων, και σε τακτικές διατήρησης υπαρχουσών blockchain βάσεων δεδομένων για την καλύτερη διασφάλιση της ακεραιότητας των δεδομένων που ανταλλάσσονται.

Προαπαιτούμενα

Αυτή η ενότητα δεν έχει κανένα προαπαιτούμενο.

Στόχοι μάθησης

- Να εξηγήσει τι είναι μια βάση δεδομένων και τα βασικά στοιχεία του τρόπου λειτουργίας της.
- Να εισαγάγει τις βασικές έννοιες της τεχνολογίας επικοινωνίας peer-to-peer (P2P) και τα πλεονεκτήματά της σε σχέση με το παραδοσιακό παράδειγμα.
- Να εξηγήσει τις μεθόδους που χρησιμοποιούνται για τη δημιουργία μιας βάσης δεδομένων σε περιβάλλον P2P (δηλαδή το blockchain).
- Να συζητήσει τις κρίσεις, τα όρια και τα μειονεκτήματα της χρήσης τεχνολογίας blockchain σε σχέση με τις κεντρικοποιημένες βάσεις δεδομένων.
- Να παρουσιάσει περιπτώσεις χρήσης στις οποίες η τεχνολογία blockchain είναι ευεργετική.

Μαθησιακά αποτελέσματα

- Να κατανοήστε τα βασικά στοιχεία του σχεδιασμού βάσης δεδομένων.
- Να κατανοήστε τους βασικούς μηχανισμούς εργασίας των δικτύων επικοινωνίας peer-to-peer.

- Να κατανοήστε γιατί η τεχνολογία blockchain αναπτύχθηκε ως λύση στα προβλήματα που αντιμετωπίζει ο σχεδιασμός κατανεμημένων βάσεων δεδομένων peer-to-peer.
- Να γνωρίσετε ποιες περιπτώσεις βάσεις δεδομένων peer-to-peer μπορεί να είναι ή να μην είναι χρήσιμες.
- Να κατανοήστε γιατί η ακεραιότητα των δεδομένων δεν αποτελεί εγγύηση για την ακρίβεια των πληροφοριών όταν εμπλέκεται ο ανθρώπινος παράγοντας.

Πρόγραμμα Εκπαίδευσης

1. Επεξήγηση του τι είναι μια βάση δεδομένων και πώς λειτουργεί
   1.1. Αρχές βάσεων δεδομένων και τρόποι λειτουργείας
   1.2. Πού είναι απαραίτητες οι βάσεις δεδομένων και γιατί απαιτείται μια νέα τεχνολογία
2. Τι είναι το peer-to-peer και πώς διαφέρει από το παραδοσιακό παράδειγμα επικοινωνίας
   2.1. Καλύτερη απόδοση στη διανομή δεδομένων και την αποκέντρωση δεδομένων
   2.2. Εξάλειψη σημείου αποτυχίας
3. Πώς να δημιουργήσετε μια αξιόπιστη βάση δεδομένων σε ένα δίκτυο P2P, το blockchain
   3.1. Πώς συνδέεται το μπλοκ πληροφοριών
   3.2. Γιατί είναι σχεδόν εγγυημένη η ακεραιότητα των δεδομένων αλυσίδας
4. Κρισιμότητα και όρια της τεχνολογίας blockchain, περιπτώσεις χρήσης στις οποίες είναι κατάλληλη ή όχι
   4.1. Γιατί είναι χρήσιμο μόνο όταν οι πληροφορίες πρέπει να ανταλλάσσονται μεταξύ πολλών κόμβων
   4.2. Καλύτερο σενάριο: πολλοί κόμβοι με έλλειψη εμπιστοσύνης
5. Επιτυχημένες πρακτικές περιπτώσεις και πιθανές μελλοντικές υλοποιήσεις
   5.1. Έλεγχος ποιότητας και έλεγχος αλυσίδας πληροφορίας
   5.2. Μεγαλύτερη διαφάνεια στο σύστημα υγειονομικής περίθαλψης

Ενότητα Μάθησης 2: Τεχνικές κρυπτογράφησης

Περιγραφή

Οι τεχνολογίες Blockchain βασίζονται σε μεγάλη ποικιλία κρυπτογραφικών τεχνικών για να διασφαλίσουν την λειτουργικότητά τους. Τα διαδοχικά μπλοκ σε ένα συνεχώς αναπτυσσόμενο blockchain συνδέονται μεταξύ τους μέσω συναρτήσεων hash. Οι λογαριασμοί σε ένα blockchain αναγνωρίζονται από κρυπτογραφικά δημόσια κλειδιά και τα αντίστοιχα ιδιωτικά κλειδιά χρησιμοποιούνται για την εξουσιοδότηση συναλλαγών. Οι τεχνικές κρυπτογράφησης είναι μία κεντρική ιδέα για την κατανόηση των DLTs γενικότερα, και ειδικότερα των blockchains.

Η δεύτερη ενότητα μάθησης εισάγει και περιγράφει σε βάθος τις κρυπτογραφικές έννοιες που είναι κεντρικές για την τεχνολογία blockchain. Οι βασικές αρχές της κρυπτογραφίας παρουσιάζονται σε μια αρχική επισκόπηση. Εισάγεται η έννοια της συνάρτησης hash και δίνονται παραδείγματα συναρτήσεων hash και των εφαρμογών τους. Συμμετρικές και ασύμμετρες τεχνικές κρυπτογραφίας συζητούνται λεπτομερώς, με παραδείγματα και συνεδρίες εργαστηρίου. Εισάγεται η έννοια του Zero-Knowledge Proof και συζητείται η εφαρμογή του στην κρυπτογραφία στο χώρο του blockchain.

Προαπαιτούμενα

Αυτή η ενότητα δεν έχει κανένα προαπαιτούμενο.

Στόχοι μάθησης

- Να εισαγάγει τα βασικά χαρακτηριστικά της κρυπτογραφίας και τις πιθανές χρήσεις της στο Blockchain.
- Να παρουσιάσει συγκριτικά διαφορετικά κρυπτοσυστήματα και την εξέλιξή τους.
- Να περιγράψει την έννοια της συνάρτησης hash και να παρουσιάσει συγκριτικά ένα σύνολο λειτουργιών hash και πώς αυτές χρησιμοποιούνται σε συστήματα που βασίζονται σε blockchain.
- Να εξηγήσει τις βασικές έννοιες των συμμετρικών και ασύμμετρων κρυπτογραφικών συστημάτων.
- Να παρουσιάσει κρυπτογραφικές τεχνικές διατήρησης απορρήτου και Zero-Knowledge Proof.
- Να δείξει πώς εφαρμόζονται οι κρυπτογραφικές τεχνικές σε συστήματα βασισμένα σε blockchain.
- Να παρουσιάσει σχετικές περιπτώσεις χρήσης που δημιουργήθηκαν γύρω από την Κρυπτογραφία Blockchain.

Μαθησιακά αποτελέσματα

- Να κατανοήστε τις βασικές έννοιες της κρυπτογραφίας.
- Να εξετάστε ποιο κρυπτοσύστημα είναι κατάλληλο ανάλογα με την περίπτωση χρήσης.
- Να προσδιορίστε και αναλύστε τις διάφορες λειτουργίες hash.

- Να προσδιορίσετε και να αναλύσετε εφαρμογές συμμετρικής και ασύμμετρης κρυπτογραφίας.
- Να συζητήσετε και αναλύσετε κρυπτογραφικές μεθόδους διατήρησης απορρήτου και Zero-Knowledge Proof.
- Να προσδιορίσετε και να αξιολογήσετε εφαρμογές κρυπτογραφικών μεθόδων σε συστήματα βασισμένα σε blockchain.
- Να εξετάσετε πώς χρησιμοποιούνται τεχνικές κρυπτογράφησης σε σχετικές περιπτώσεις χρήσης blockchain.

Πρόγραμμα Εκπαίδευσης

1. Εισαγωγή στην Κρυπτογραφία
   1.1. Τι είναι η κρυπτογραφία;
   1.2. Ταξινόμηση κρυπτοσυστημάτων
   1.3. Βασικές αρχές
   1.4. Κύρια κρυπτοσυστήματα και εξέλιξη
   1.5. Τέλειες συνθήκες κρυπτογράφησης
   1.6. Κρυπτοανάλυση
2. Λειτουργίες κατακερματισμού
   2.1. Τι είναι η συνάρτηση Hash;
   2.2. Τύποι λειτουργιών Hash: MD5, SHA-x
   2.3. Εργαστήριο: πειραματισμός με λειτουργίες κατακερματισμού
3. Συμμετρική κρυπτογραφία
   3.1. Ορισμός
   3.2. Κρυπτογράφηση Vernam, Flow και Block
4. Ασύμμετρη κρυπτογραφία
   4.1. Ορισμός
   4.2. Βασικοί αλγόριθμοι ανταλλαγής (Diffie-Hellman)
   4.3. RSA
5. Εργαστήριο: πειραματισμός με συμμετρική και ασύμμετρη κρυπτογράφηση
6. Αποδείξεις μηδενικής γνώσης (Zero-Knowledge Proof)
7. Εφαρμογές της Κρυπτογραφίας Blockchain
   7.1. Εφαρμογή σε ανταλλαγές QR
   7.2. Διαχείριση διευθύνσεων Bitcoin και Ethereum
   7.3. Πρακτική της θεωρίας μπλοκ
8. Περίπτωση χρήσης: Τομέας χρηματοδότησης, υγεία, νομικές υπηρεσίες, άμυνα, δημόσια διοίκηση, βιομηχανική Ψηφιοποίηση, Κοινωνικά Έργα, Αντιμετώπιση της φτώχειας, Διαχείριση ατομικής ταυτότητας

Γνωστική Ενότητα 3: Μηχανισμοί Συναίνεσης

Περιγραφή

Ένα από τα κεντρικά (σημαντικά) προβλήματα στη σχεδίαση ενός συστήματος blockchain είναι η επιλογή του μηχανισμού που θα χρησιμοποιηθεί από τους κόμβους του δικτύου (nodes) για να επιτευχθεί συμφωνία/συναίνεση (consenus) για την κατάσταση του δικτύου με αποκεντρωμένο (decentralized) τρόπο, δηλαδή χωρίς να υπάρχει μια κεντρική έμπιστη οντότητα (αρχή, party).

Η Γνωστική Ενότητα 3 εξερευνά τους υπάρχοντες (τωρινούς, τρέχοντες) μηχανισμούς οι οποίοι διαχειρίζονται την επίτευξη συμφωνίας (handle the agreement) μεταξύ όλων των κόμβων/χρηστών (nodes) που συμμετέχουν σε ένα σύστημα Blockchain. Θα συζητηθούν οι πιο συχνά χρησιμοποιούμενοι μηχανισμοί συναίνεσης, δίνοντας έμφαση τόσο στην τεχνολογική όσο και στην επιχειρηματική σκοπιά του θέματος.

Η ενότητα ξεκινά με την επεξήγηση της ανάγκης χρήσης ενός μηχανισμού συναίνεσης σε μια κατανεμημένη βάση δεδομένων και παρουσιάζει δυνατές λύσεις πάνω σε permissioned συστήματα. Παρουσιάζεται ο ρόλος της θεωρίας Παιγνίων (Game theory) στη σχεδίαση των μηχανισμών συναίνεσης. Ακολουθεί μια κατηγοριοποίηση των διαφορετικών μηχανισμών συναίνεσης που έχουν υλοποιηθεί στην πράξη ή έχουν προταθεί στη βιβλιογραφία σε δυο ευρείες κατηγορίες, οι μηχανισμοί Proof of Work και οι μηχανισμοί Proof of Stake, και γίνεται αναφορά σε ενδεχόμενες επιθέσεις σε τέτοιους μηχανισμούς. Έπειτα, δίνεται μια απεικόνιση των συμβιβασμών (trade-offs) μεταξύ της ανταμοιβής για την συντήρηση/διατήρηση (maintain) του Blockchain και της ασφάλειας εναντίον κακόβουλων επιθέσεων οι οποίες μπορούν να διακινδυνέψουν (θέσουν σε κίνδυνο) την ακεραιότητα του/ενός συστήματος/Blockchain. Δίνεται έμφαση στον βαθμό της αποκέντρωσης των μηχανισμών που παρουσιάζονται. Τέλος, παρουσιάζεται μια σειρά από πρακτικά σενάρια χρήσης (case studies).

Οι συμμετέχοντες που θα ολοκληρώσουν τη Γνωστική Ενότητα 3 θα είναι σε θέση να αντιληφθούν τα προτερήματα και μειονεκτήματα των διάφορων μηχανισμών συναίνεσης στο πλαίσιο οποιοδήποτε επιχειρηματικού σχεδίου (business plan) το οποίο θα βασίζεται σε κατανεμημένη βάση δεδομένων (distributed ledger), καθώς και τους περιορισμούς όσον αφορά την ακρίβεια, την αποδοτικότητα του κόστους (cost efficiency), τον βαθμό της αποκέντρωσης, την επεκτασιμότητα, την ταχύτητα και τη βιωσιμότητα του δικτύου.

Προαπαιτούμενα

Η Γνωστική Ενότητα 3 έχει ως προαπαιτούμενα:

- Σχεδίαση ομότιμης βάσης δεδομένων (peer-to-peer database) (Γ.Ε.1)
- Τεχνικές κρυπτογράφησης (Γ.Ε.2)

Μαθησιακοί Στόχοι

- Να εξηγηθεί η ανάγκη χρήσης ενός μηχανισμού συναίνεσης σε ένα σύστημα που βασίζεται σε blockchain

- Να παρουσιαστούν οι μηχανισμοί συναίνεσης που χρησιμοποιούνται σε permissioned blockchain.
- Να συζητηθεί ο ρόλος της Θεωρίας Παιγνίων στη σχεδίαση ενός μηχανισμού συναίνεσης
- Να παρουσιαστούν τα πρωτόκολλα συναίνεσης Proof-of-Concept (PoX) που χρησιμοποιούνται πιο συχνά σε blockchain συστήματα.
- Να συζητηθούν ενδεχόμενες επιθέσεις σε κατανεμημένα πρωτόκολλα συναίνεσης.
- Να γίνει περιγραφή για τις πιθανές ανταμοιβές που χρησιμοποιούνται σε κατανεμημένα πρωτόκολλα συναίνεσης.
- Να παρουσιαστούν επιθέσεις σε πρωτόκολλα συναίνεσης που σχετίζονται με τις ανταμοιβές.
- Να συζητηθούν τα κόστη χρήσης των πιο συχνά χρησιμοποιούμενων κατανεμημένων πρωτοκόλλων συναίνεσης.
- Να συζητηθούν η απόδοση και επεκτασιμότητα των πιο συχνά χρησιμοποιούμενων κατανεμημένων πρωτοκόλλων συναίνεσης.
- Να παρουσιαστούν εναλλακτικές λύσεις των θεμάτων επεκτασιμότητας των κατανεμημένων πρωτοκόλλων συναίνεσης που χρησιμοποιούνται σε Blockchain συστήματα.
- Να παρουσιαστούν σενάρια χρήσης διαφορετικών κατανεμημένων μηχανισμών συναίνεσης σε διαφορετικά Blockchain συστήματα.

Μαθησιακά Αποτελέσματα

- Κατανόηση του ρόλου της συναίνεσης σε Blockchain συστήματα. • Κατανόηση της λειτουργίας των PoX κατανεμημένων πρωτοκόλλων συναίνεσης.
- Κατανόηση σχετικά με ενδεχόμενες επιθέσεις στα κατανεμημένα πρωτόκολλα συναίνεσης.
- Σύγκριση σχετικά με το κόστος, την απόδοση, την επεκτασιμότητα και την ασφάλεια των διαφόρων πρωτοκόλλων συναίνεσης αναλύοντας τις προδιαγραφές σχεδίασης.
- Εκτίμηση των επιθυμητών χαρακτηριστικών ενός πρωτοκόλλου συναίνεσης για ένα συγκεκριμένο επιχειρηματικό μοντέλο.

Περίληψη

1. Εισαγωγή
   1.1. Η ανάγκη χρήσης μηχανισμού συναίνεσης
   1.2. Permissioned Blockchains: Συναίνεση μέσω του Byzantine-Fault Tolerant (BFT) μηχανισμού ψηφοφορίας
2. Ο ρόλος της Θεωρία Παιγνίων στην συναίνεση
3. Πρωτόκολλα Proof-of-Concept (PoX)
   3.1. Η έννοια του πιθανοκρατικής συναίνεσης και οι ιδιότητές της
   3.2. Κρυπτογραφικοί γρίφοι λοταρίας (Cryptographic puzzle lotteries) και οι απαιτούμενες ιδιότητες τους
   3.3. Κύρια πρωτόκολλα: Proof-of-Work, Proof-of-Stake, Εξουσιοδοτούμενα Proof-of-Work, Proof-ofAuthority
   3.4. αξινόμηση ενδεχόμενων επιθέσεων: Sybil attacks, race attacks, Finney attacks, 51% attacks.
4. Ανταμοιβές

4.1. Βασική Θεωρία: Χαμένο κόστος (Sunk Cost), Πρόβλημα εντολέα-εντολοδόχου (Principal-agent problems), Συμβατότητα ανταμοιβών (incentive compatibility)
4.2. Συμβατότητα ανταμοιβών στα PoX πρωτόκολλα: tokens, mining pools, mining cartels
4.3. Αγορές με tokens
4.4. Αδυναμίες των PoX πρωτοκόλλων: selfish mining, block withholding, lie-in-wait mining pools, pool hopping

5. Κόστος
   5.1. Η κοστοβόρα φύση των PoX πρωτοκόλλων
   5.2. Το Proof-of-Stake (PoS) πρωτόκολλο και η τραγωδία των συνηθισμένων προβλημάτων
   5.3. Θέματα ασφάλειας στα PoX πρωτόκολλα: nothing-at-stake attacks. Grinding attacks
6. Απόδοση
   6.1. Η περιορισμένη απόδοση των permissionenless blockchains
   6.2. Υβριδικά πρωτόκολλα
   6.3. Διαλειτουργικότητα μεταξύ blockchain
   6.4. Μη-γραμμικά δίκτυα Blockchain: το πρωτόκολλο Greedy Heaviest-Observed Sub-Tree (GHOST)
   6.5. Πρωτόκολλα βασισμένα σε Direct Acyclic Graph (DAG)
7. Παραδείγματα
   7.1. Hyperledger Fabric (BFT)
   7.2. Bitcoin (PoW)
   7.3. Primecoin (PoUS)
   7.4. Filecoin (UPoW)
   7.5. SpaceMint (PoSP)
   7.6. Bytecent (PoH)
   7.7. Peercoin (PoS)
   7.8. Algorand (Hybrid protocols)
   7.9. Teechain on Bitcoin (Side-chain networks)
   7.10. Ethereum Casper implementation (GHOST)

Γνωστική Ενότητα 4: Ψηφιακές Υπογραφές

Οι Ψηφιακές Υπογραφές είναι η επέκταση των χάρτινων υπογραφών στον ψηφιακό κόσμο, οπού καθίσταται εφικτό λόγω της ανάπτυξης της ασύμμετρης κρυπτογραφίας. Όπως και οι πραγματικές υπογραφές, είναι ένας τρόπος απόδειξης της ταυτότητας κάποιου, και τρόπος επιβεβαίωσης της προέλευσης ενός μηνύματος.

Η Γνωστική Ενότητα 4 περιγράφει τις ιδιότητες και τις τεχνικές απαιτήσεις που χρειάζονται για την υλοποίηση των ψηφιακών υπογραφών, και το μαθηματικό υπόβαθρο. Τα γενικά χαρακτηριστικά των αλγορίθμων ψηφιακών υπογραφών έπειτα παρουσιάζονται, και συζητούνται εκτενώς συγκεκριμένοι αλγόριθμοι που συχνά χρησιμοποιούνται σε υλοποιήσεις συστημάτων blockchain. συζητούνται αλγόριθμοι ψηφιακών υπογραφών που διατηρούν την ιδιωτικότητα, με επίκεντρο την χρήση τους στον χώρο των κρυπτονομισμάτων, και παρουσιάζονται οι έννοιες της Ανωνυμίας και της Ψευδωνυμίας των συναλλαγών σε ένα blockchain. Αναλογίζεται η ασφάλεια των ψηφιακών υπογραφών και τα πιθανά σενάρια επίθεσης, και μέσα σε εργαστήρι της Ενότητας, αναλύεται εις βάθος ένα πιθανό διάνυσμα επίθεσης. Το τελευταίο κομμάτι της Ενότητας συζητά το μέλλον των ψηφιακών υπογραφών, παρουσιάζοντας νέους αλγορίθμους που σχεδιάστηκαν για να είναι ανθεκτικοί σε τωρινές και μελλοντικές απειλές – συνδεμένες με την επέλαση των κβαντικών υπολογιστών.

Προαπαιτούμενα

Αυτή η γνωστική ενότητα έχει τα εξής προαπαιτούμενα:

- Τεχνικές Κρυπτογράφησης (LM2)

Μαθησιακοί Στόχοι

- Να εξηγηθούν οι βασικές ιδιότητες που πρέπει να διατηρεί μια ψηφιακή υπογραφή.
- Να παρουσιαστούν οι αλγόριθμοι ψηφιακών υπογραφών που χρησιμοποιούνται πιο συχνά σε συστήματα βασισμένα σε blockchain.
- Να παρουσιαστούν αλγόριθμοι ψηφιακών υπογραφών που διατηρούν την ιδιωτικότητα.
- Να συζητηθούν οι δυνατότητες ανωνυμίςα και ψευδωνυμίας σε συστήματα blockchain.
- Να παρουσιαστούν επιθέσεις και θέματα ασφάλειας σχετικά με αλγορίθμους ψηφιακών υπογραφών.
- Να παρουσιαστούν οι πλέον καινοτόμες εξελίξεις αλγορίθμων ψηφιακών υπογραφών.
- Να παρουσιαστούν Περιπτώσεις Χρήσης ψηφιακών υπογραφών σε συστήματα blockchain.

Μαθησιακά Αποτελέσματα

- Να κατανοηθούν οι θεμελιώδεις ιδιότητες των αλγορίθμων ψηφιακών υπογραφών.
- Να κατανοηθούν λεπτομέρειες για τους πιο συχνούς αλγορίθμους ψηφιακών υπογραφών
- Να αποκτηθούν τεχνικές ικανότητες σχετικές με τη χρήση ψηφιακών υπογραφών.
- Να κατανοηθεί η λειτουργία των αλγορίθμων ψηφιακών υπογραφών που διατηρούν την ιδιωτικότητα.
- Να απαριθμηθούν πιθανές επιθέσεις σε συχνούς αλγορίθμους ψηφιακών υπογραφών.
- Περιγραφή

Περίληψη

1. Ορισμοί Υπογραφών, ιδιότητες και αιτήσεις

2. Εισαγωγικά
   2.1. Ελλειπτικές Καμπύλες
   2.2. Εργαστήρι: η βιβλιοθήκη bitcoin-core/secp256k1

3. Αλγόριθμοι ψηφιακών υπογραφών
   3.1. Εισαγωγή
   3.2. DSA
   3.3. ECDSA
   3.4. Υπογραφές Schnorr
   3.5. Εργαστήρι: εφαρμογή και ανάλυση υπογραφών Schnorr

4. Υπογραφές τοπολογίας δακτυλίου
   4.1. Ιδιότητες
   4.2. Ο ρόλος υπογραφών δακτυλίου στο Monero blockchain
   4.3. Εργαστήρι: εφαρμόζοντας υπογραφές δακτυλίου

5. Ανωνυμία και ψευδωνυμία σε συναλλαγές blockchain

6. Ασφάλεια και Επιθέσεις
   6.1. Επισκόψηση προβλημάτων ασφάλειας και επιθέσεων
   6.2. Εργαστήρι: συγκεκριμένες επιθέσεις σε υπογραφές Schnorr

7. Το Μέλλον των Ψηφιακών Υπογραφών: Πλέγματα, υπογραφές Κατακερματισμού, και υπογραφές Κατωφλιού
8. Περιπτώσεις χρήσης

Γνωστική Ενότητα 5: Έξυπνα Συμβόλαια

Περιγραφή

Ο όρος "Έξυπνα Συμβόλαια χρησιμοποιείται με δύο διαφορετικές σημασίες:

- "Ενα Έξυπνο Συμβόλαιο είναι ένα σύνολο κώδικα (οι Μέθοδοί του) και δεδομένων (η Κατάστασή του) που "κατοικεί" σε μια συγκεκριμένη διεύθυνση πάνω στο blockchain.
- "Ενα Έξυπνο Συμβόλαιο (ως Συμβόλαιο) είναι ένα ηλεκτρονικό πρωτόκολλο με σκοπό την ψηφιακή διενέργεια, την επαλήθευση ή την επιβολή των όρων τ ης πραγματοποίησης ενός συμβολαίου."

Η Γνωστική Ενότητα 5 εξερευνά θέματα σχεδίασης εφαρμογών πάνω σε blockchain (ήτοι: Έξυπνων Συμβολαίων) που μπορούν να εκτελέσουν αυτόματα τους όρους ενός συμβολαίου, και εστιάζει τόσο στο Τεχνολογικό όσο και στο Επιχειρηματικό κομμάτι του θέματος.

Η ενότητα ξεκινά με μια εισαγωγή στην έννοια του Έξυπνου Συμβολαίου και με περιγραφή της ιστορικής τους ανάπτυξης. Παρουσιάζεται μία γενική περιγραφή των γλωσσών προγραμματισμού που χρησιμοποιούνται για την ανάπτυξη Έξυπνων Συμβολαίων για συστήματα blockchain, μαζί με τα περιβάλλοντα εκτέλεσής τους. Ακολουθεί μια εκτενής περιγραφή της Εικονικής Μηχανής του Ethereum (Ethereum Virtual Machine – EVM) και ένα θεματικό εργαστήριο στην ανάπτυξη Έξυπνων Συμβολαίων στην πλατφόρμα του Ethereum, χρησιμοποιώντας τη γλώσσα Solidity. Συζητούνται εκτενώς οι Μάντεις (Oracles), μια ειδική κατηγορία Έξυπνων Συμβολαίων που επικοινωνούν με έμπιστες οντότητες. συζητούνται οι έννοιες του Κόστος Υπολογισμού και των ζητημάτων ασφαλείας του προγραμματισμού Έξυπνων Συμβολαίων, και προτείνονται βέλτιστες τακτικές για την ελαχιστοποίηση των προβλημάτων και ρίσκων που συναντώνται. Τέλος, συζητούνται και περιγράφονται τα κύρια νομικά και ρυθμιστικά θέματα που θα πρέπει να εξερευνηθούν για να πλαισιωθεί η λειτουργεία και χρήση των Έξυπνων Συμβολαίων.

Προαπαιτούμενα

Αυτή η γνωστική ενότητα έχει τα εξής προαπαιτούμενα:

- Μηχανισμοί Συναίνεσης (LM3)
- Ψηφιακές Υπογραφές (L M4)

Μαθησιακοί Στόχοι

- Να οριστούν και να επεξηγηθούν οι βασικές ιδιότητες ενό ς Έξυπνου Συμβολαίου.
- Να παρουσιαστούν διαφορετικές γλώσσες προγραμματισμού για Έξυπνα Συμβόλαια, και τα περιβάλλοντα εκτέλεσής αυτών.
- Να περιγραφεί το Ethereum blockchain και η Εικονική Μηχανή (Virtual Machine) του Ethereum.
- Να εξηγηθεί το πως χρησιμοποιείται η γλώσσα Solidity για την ανάπτυξη ενός Έξυπνου Συμβολαίου για το Ethereum Blockchain.
- Να παρουσιαστεί η έννοια των Μαντών (Oracles) και οι βασικές ιδιότητες της λειτουργίας τους.

- Να συζητηθεί το υπολογιστικό κόστος της *παράταξης* (deployment) και της εκτέλεσης ενός Έξυπνου Συμβολαίου και το ρόλο του Gas μέσα στο Ethereum Blockchain.
- Να συζητηθούν θέματα ασφάλειας σχετικά με την ανάπτυξη και τη χρήση Έξυπνων Συμβολαίων.
- Να παρουσιαστούν τα νομικά πλαίσια που επηρεάζουν τη χρήση των Έξυπνων Συμβολαίων.
- Να παρουσιαστούν τα νομικά θέματα σχετικά με τη χρήση Έξυπνων Συμβολαίων σε ένα σύστημα βασισμένο σε blockchain.

Μαθησιακά Αποτελέσματα

- **Να περιγραφούν** οι βασικές έννοιες των Έξυπνων Συμβολαίων.
- **Να αναγνωριστούν** οι διαφορετικές γλώσσες προγραμματισμού για Έξυπνα Συμβόλαια και τα περιβάλλοντα εκτέλεσής τους.
- **Να αναγνωριστούν** τα χαρακτηριστικά-κλειδιά των διαφόρων γλωσσών Έξυπνων Συμβολαίων.
- **Να περιγραφεί** το Ethereum Blockchain.
- **Να εξηγηθεί** πως λειτουργεί το Ethereum Virtual Machine.
- **Να υλοποιηθούν** Έξυπνα Συμβόλαια σε Ethereum χρησιμοποιώντας τη γλώσσα Solidity
- **Να εξεταστεί** το υπολογιστικό κόστος της παράταξης και χρήσης Έξυπνων Συμβολαίων σε Ethereum.
- **Να παρουσιαστούν** περιπτώσεις χρήσης Έξυπνων Συμβολαίων σε πολλαπλούς κλάδους.
- **Να γίνουν αντιληπτές** οι τρέχοντες περιορισμοί και όρια της τεχνολογίας.
- **Να αναγνωριστούν** θέματα και προβληματικές σε σχέση με τ ην ανάπτυξη Έξυπνων Συμβολαίων.
- **Να εξεταστούν** προτερήματα και μειονεκτήματα της χρήσης Έξυπνων Συμβολαίων.
- **Να αναγνωριστούν** προβληματισμοί σχετικά με την ασφάλεια, τη σταθερότητα και το κόστος ενός Έξυπνου Συμβολαίου.
- **Να αξιολογηθεί** εάν μια λύση Έξυπνου Συμβολαίου είναι κατάλληλο για το μελετηθέν πρόβλημα.
- **Να αξιολογηθεί** το πως και γιατί να εφαρμοστούν Έξυπνα Συμβόλαια σε πραγματικές εφαρμογές.
- **Να εφαρμοστούν** Έξυπνα Συμβόλαια σε πραγματικές εφαρμογές, πραγματικού κόσμου.

Περίληψη

1. Εισαγωγή στα Έξυπνα Συμβόλαια
   1.1. Βασικοί ορισμοί Έξυπνων Συμβολαίων
   1.2. Που εκτελείται ένα Έξυπνο Συμβόλαιο?
   1.3. Κατανοώντας την Εικονική Μηχανή (Virtual Machine) ενός Blockchain
   1.4. Βλέποντας τον πηγαίο κώδικα ενός Έξυπνου Συμβολαίου
   1.5. Χρήσιμη Ορολογία & Έννοιες στα Έξυπνα Συμβόλαια
   1.6. Βέλτιστες πρακτικές κατά τη χρήση Έξυπνων Συμβολαίων

2. Εισαγωγή σε Έξυπνα Συμβόλαια Ethereum και στο Ethereum Virtual Machine (EVM)
   2.1. Επικράτηση του Ethereum blockchain στην ανάπτυξη Έξυπνων Συμβολαίων
   2.2. Ether και Gas: Το κόστος εκτέλεσης ενός Έξυπνου Συμβολαίου

2.3 Παίρνοντας μια γεύση: Λειτουργικά παραδείγματα Έξυπνων Συμβολαίων σε Ethereum
2.4 Πολλαπλά Έξυπνα Συμβόλαια σε ταυτοχρονισμό

3. Εμπιστοσύνη, Ασφάλεια και Αποδοτικότητα Έξυπνων Συμβολαίων "στο πεδίο"
   3.1. Επιπτώσεις στην Αγορά και επιστημονική καινοτομία των Έξυπνων Συμβολαίων
   3.2. Κατανοώντας την Εμπιστοσύνη
   3.3. Κατασκευάζοντας συστήματα ανθεκτικά στον χρόνο μέσω Έξυπνων Συμβολαίων
   3.4. Η διπλή σημασία της Ασφάλειας στα Έξυπνα Συμβόλαια
   3.5. Καινοτομία των Έξυπνων Συμβολαίων
   3.6. Διάσημα σκάνδαλα και επιθέσεις σχετικά με Έξυπνα Συμβόλαια

4. Γλώσσες προγραμματισμού Έξυπνων Συμβολαίων και Περιβάλλοντα Εκτέλεσης
   4.1. Γράφοντας Έξυπνα Συμβόλαια
   4.2. Η ροή εργασίας για την ανάπτυξη ενός Έξυπνου Συμβολαίου
   4.3. Η ευθύνη του προγραμματιστή ως προς την συγγραφή ενός Έξυπνου Συμβολαίου
   4.4. Κόστος λειτουργίας Έξυπνων Συμβολαίων
   4.5. Οι διαφορετικές πλατφόρμες ανάπτυξης Έξυπνων Συμβολαίων και οι διαφορές τους
   4.6. Επιλέγοντας το σωστό blockchain για σένα: Που να αναπτύξεις το Έξυπνο Συμβόλαιό σου

5. Αναπτύσσοντας Έξυπνα Συμβόλαια στο Ethereum blockchain
   5.1. Η γλώσσα Solidity: Μια αντικειμενοστραφής, υψηλού-επιπέδου γλώσσα για Έξυπνα Συμβόλαια
   5.2. Σχεδιάζοντας ένα Έξυπνο Συμβόλαιο σε Solidity
   5.3 Λειτουργικά παραδείγματα Έξυπνων Συμβολαίων σε Solidity

6. Υπηρεσίες Μαν των (Oracles)
   6.1. Ορισμός ενός blockchain Oracle: Τι είναι, Τι κάνουν
   6.2. Εγχέοντας πιστοποιήσιμα δεδομένα μέσα στο blockchain
   6.3. "Μποτιλιαρίσματα" επικέντρωσης λόγω υπηρεσιών Oracle
   6.4. Αποκεντρωμένες Υπηρεσίες Oracle

7. Ζητήματα Ασφαλείας σε Έξυπνα Συμβόλαια & επιπτώσεις
   7.1. Μεταβαίνοντας από Εμπιστοσύνη-σε-Ανθρώπους σε Εμπιστοσύνη-σε-Κώδικα
   7.2. Μονιμότητα δεδομένων σε συναλλαγές Έξυπνων Συμβολαίων
   7.3. Επιλεκτική-αφάνεια σε δεδομένα Έξυπνων Συμβολαίων
   7.4. Κβαντική ετοιμότητα του Έξυπνου Συμβολαίου σου
   7.5. Ευθύνη του Δημιουργού κατά τη δημιουργία ενός Έξυπνου Συμβολαίου
   7.6. Τέλος Κύκλου Ζωής Έξυπνου Συμβολαίου: παραμένοντας ευκίνητοι
   7.7. Τα *Forks* (Hard & Soft) και αντίμετρα της κοινότητας εναντίον επιθέσεων σε Έξυπνα Συμβόλαια

8. Πραγματικά σενάρια χρήσης Έξυπνων Συμβολαίων (Περιπτώσεις Χρήσης)
   8.1. Τα Έξυπνα Συμβόλαια στρωμένα στη δουλειά – Περιπτώσεις χρήσης πραγματικού κόσμου
   8.2. Το παράδειγμα του Μυρμηγκιού στην Μυρμηγκοφωλιά: Προγραμματιστές που ψάχνουν την καλύτερη πλατφόρμα για να γράψουν τα Έξυπνα Συμβόλαιά τους.
   8.3. Starting opportunities: Dev contests, bounties, funding for Smart Contract projects

9. Τα Έξυπνα Συμβόλαια στις Επιχειρήσεις
   9.1. Πως τα Έξυπνα Συμβόλαια εξυψώνουν την Ευρωπαϊκή και Διεθνή επιχειρηματική αρένα
   9.2. Ένα πρακτικό σενάριο: Διαχείριση Αγροτικής Εφοδιαστικής Αλυσίδας μέσω Έξυπνων Συμβολαίων

9.3. Ευκαιρίες χρηματοδότησης για την υποστήριξη της υλοποίησης συστημάτων Έξυπνων Συμβολαίων στην Ευρώπη
9.4. Νομικό Υπόβαθρο για τη χρήση Έξυπνων Συμβολαίων
9.5. Μεγάλης-κλίμακας Επιθέσεις και hacks: Κίνδυνοι στη χρήση Έξυπνων Συμβολαίων

Ενότητα Μάθησης 6: Απόρρητο και δικαιώματα ιδιοκτησίας

Περιγραφή

Στις περισσότερες περιπτώσεις, οι τεχνολογικές εξελίξεις βρίσκονται μπροστά από τις ρυθμίσεις και τη νομοθεσία και τόσο η κοινωνία όσο και η νομοθεσία πρέπει να καλύψουν τη διαφορά και να προσαρμοστούν σε νέες καταστάσεις όπως αυτές ορίζονται από την τεχνολογία. Σε σπάνιες περιπτώσεις, ωστόσο, η τεχνολογία έρχεται να βοηθήσει τη νομοθεσία και την κοινωνία, και, επιτρέπει μεγαλύτερη διαφάνεια και μεγιστοποίηση της ταχύτητας στις αλυσίδες πληροφορίας. Η έκτη ενότητα μάθησης περιγράφει τους τρόπους με τους οποίους η τεχνολογία blockchain μπορεί να υποστηρίξει τη νομοθεσία για τα δικαιώματα ιδιοκτησίας και τα ζητήματα που σχετίζονται με το απόρρητο. Σε αυτή την ενότητα μάθησης εξηγείται η ευρωπαϊκή νομοθεσία για τα δικαιώματα ιδιοκτησίας και πώς οι τεχνολογίες blockchain θα μπορούσαν να βοηθήσουν στο σχεδιασμό στρατηγικών διαφάνειας. Το GDPR και τα ζητήματα που σχετίζονται με το απόρρητο θα συζητηθούν στη συνέχεια μαζί με συνέπειες που σχετίζονται με το αμετάβλητο της τεχνολογίας blockchain (όπως για παράδειγμα το δικαίωμα στη λήθη). Τέλος, οι τεχνολογίες για την ενίσχυση του απορρήτου που βασίζονται σε blockchain θα συζητηθούν λεπτομερώς.

Προαπαιτούμενα

Αυτή η εκπαιδευτική ενότητα έχει τις ακόλουθες προϋποθέσεις:

- Εισαγωγή στα θέματα DLT (LM0)
- Έξυπνα Συμβόλαια (LM5).

Στόχοι μάθησης

- Να παρουσιαστεί το ισχύον ευρωπαϊκό νομοθετικό πλαίσιο σχετικά με τα δικαιώματα ιδιοκτησίας.
- Να επεξηγηθούν οι υπάρχοντες τύποι αδειών χρήσης λογισμικού.
- Να εξηγήσει τους διεθνείς νόμους περί πνευματικών δικαιωμάτων.
- Να συζητήσει τον συντονισμό των αδειών και τον ρόλο των μητρώων.
- Να συζητήσει θέματα που σχετίζονται με τα δικαιώματα ιδιοκτησίας που προκύπτουν κατά την εφαρμογή DLT.
- Να παρουσιάσει τον νόμο GDPR και τις συνέπειές του στην προστασία της ιδιωτικής ζωής και της πληροφορίας.
- Να συζητήσει θέματα που σχετίζονται με το GDPR που προκύπτουν κατά τη χρήση DLT.
- Να παρουσιάσει ένα σύνολο τεχνικών κρυπτογράφησης προστασίας προσωπικών δεδομένων.
- Να συζητήσει ζητήματα που σχετίζονται με το απόρρητο που προκύπτουν σε ένα σύστημα που βασίζεται σε DLT.

Μαθησιακά αποτελέσματα

- Να κατανοήστε το GDPR και τις επιπτώσεις του στις τεχνολογίες blockchain.
- Να κατανοήστε τον τρόπο εφαρμογής του νόμου κατά τη χρήση της τεχνολογίας blockchain.
- Να μάθετε τα δικαιώματα ιδιοκτησίας και πώς αυτά μπορούν να προστατευτούν χρησιμοποιώντας το blockchain.
- Να κατανοήστε πώς μπορούν να είναι τα προσωπικά δεδομένα στον έλεγχο των ατόμων χάρη στις τεχνολογίες blockchain.
- Να περιγράψτε πώς οι Angel Investors μπορούν να εκτιμήσουν εταιρείες που σχετίζονται με το Blockchain.
- Να μάθετε το ρόλο των δικαιωμάτων πνευματικής ιδιοκτησίας στην ενθάρρυνση της καινοτομίας και της δημιουργικότητας και πώς μπορεί το blockchain να διευκολύνει τα δικαιώματα πνευματικής ιδιοκτησίας
- Να κατανοήστε πώς μπορούν να προστατευθούν τα δικαιώματα ιδιοκτησίας χρησιμοποιώντας την τεχνολογία blockchain.
- Να εξετάστε θέματα ασφάλειας και απορρήτου στην αλυσίδα αποθήκευσης πληροφορίας.

Πρόγραμμα Εκπαίδευσης

1. Δικαιώματα ιδιοκτησίας
   1.1. Η νομοθεσία περί των δικαιωμάτων πνευματικής ιδιοκτησίας
   1.2. Τι είναι η άδεια χρήσης λογισμικού
   1.3. Τύποι άδειας
   1.4. Διεθνής νομοθεσία περί πνευματικών δικαιωμάτων
   1.5. Το token ως άδεια;
   1.6. Ιδιωτική παραγγελία
   1.7. Κατακερματισμός
   1.8. Συντονισμός αδειών
   1.9. Μητρώα
   1.10. Τυπικότητα
   1.11. Ορφανές εργασίες και ο δημόσιος χώρος
   1.12. 1.12.Πληροφορίες διαχείρισης δικαιωμάτων
   1.13. 1.13.Δίκαιη αμοιβή
2. Θέματα DLT σχετικά με τα δικαιώματα ιδιοκτησίας
3. GDPR - Ζητήματα με το απόρρητο και την Ελευθερία των Πληροφοριών
4. Θέματα DLT που σχετίζονται με το GDPR
5. Εφαρμοσμένες τεχνικές κρυπτογράφησης για το απόρρητο
   5.1. Λειτουργίες κατακερματισμού χαμαιλέοντα
   5.2. Διευθύνσεις Stealth
   5.1. Εμπιστευτικές συναλλαγές μέσω υπογραφών δακτυλίου
   5.2. Εφαρμογή απορρήτου μέσω απόδειξης μηδενικής γνώσης
   5.3. Ιδιωτικά έξυπνα συμβόλαια – Enigma

Ενότητα μάθησης 7: Αποκεντρωμένες Εφαρμογές βασισμένες στην τεχνολογία Blockchain

Περιγραφή

Οι Αποκεντρωμένες Εφαρμογές (Decentralized applications) διαφέρουν από τις εναλλακτικές Κεντρικές (centralized) καθώς ενισχύουν τα ομότιμα (Peer-to-peer) των συμμετεχόντων. Η ανάγκη επικοινωνίας μεταξύ μερών για επικοινωνία χωρίς την αναγκαιότητα κεντρικής αρχής είναι ένα κοινό θέμα συζήτησης και αξιολόγησης αναμεταξύ των ενδιαφερομένων για την τεχνολογία. Τέτοιες Αποκεντρωμένες εφαρμογές (dApps), μπορούν να ενδιαφέρουν διάφορες βιομηχανίες, οι οποίες μπορούν να παρουσιαστούν σαν περιπτώσεις χρήσης (use cases) π.χ. στα Χρηματοοικονομικά, Ακαδημαϊκά, στην Αλυσίδα Εφοδιασμού στα Ενεργειακά και σε άλλους τομείς.

Σε αυτή την ενότητα, θα αναλυθούν οι Εφαρμογές της τεχνολογίας σε όλες τις πτυχές, από την τεχνική αλλά και την μη τεχνική άποψη, καταρτισμένη για όλα τα είδη κοινού, με στόχο το μάθημα να είναι προσιτό και ενδιαφέρον. Ο κύριος στόχος της ενότητας είναι να βοηθήσει τους συμμετέχοντες να αξιολογήσουν ποιοι τομείς και βιομηχανίες είναι έτοιμες να υιοθετήσουν την τεχνολογία του Blockchain και ποιες είναι έτοιμες να επεκτείνουν την δραστηριότητα τους. Η αποκέντρωση και η αποδιαμεσολάβηση είναι νέες έννοιες και είναι δύσκολο να κατανοηθούν πλήρως. Υπάρχουν πολλά στοιχεία που πρέπει να ληφθούν υπόψη, όπως ο βαθμός ασφάλειας, ιδιωτικότητας και δια-λειτουργικότητας. Κάθε δίκτυο DLT ποικίλλει στο βαθμό ικανοποίησης αυτών των στοιχείων. Είναι ύψιστης σημασίας για τους δημιουργούς περιεχομένου να αξιολογήσουν τις βέλτιστες πρακτικές και τις πιθανές ελλείψεις της τεχνολογίας. Η βασική δομή και τα κύρια σχέδια σχεδιασμού των Εφαρμογών (dApps) παρουσιάζονται ως εισαγωγή στα βασικά στοιχεία της ανάπτυξης των εφαρμογών (dApps). Περιπτώσεις χρήσης της τεχνολογίας (use cases) για προηγμένες Εφαρμογές της τεχνολογίας (dApps) σε διάφορους τομείς που παρουσιάζονται μαζί με τη σχέση τους με άλλες διαταραχές τεχνολογίας στο πλαίσιο της 4ης βιομηχανικής επανάστασης.

Προαπαιτούμενα

Η ενότητα έχει ως προαπαιτούμενες τις ακόλουθες ενότητες:

- Εισαγωγή στο μάθημα και στον κόσμο των DLTs (LM0)
- Έξυπνα Συμβόλαια (LM5)

Στόχοι μαθήματος

- Η σύγκριση της χρήσης παραδοσιακών κεντρικών μοντέλων και των Αποκεντρωμένων εφαρμογών (dApps) και που μπορούν να χρησιμοποιηθούν
- Η συσχέτιση των βασικών χαρακτηριστικών των Αποκεντρωμένων εφαρμογών (dApps) με τις θεμελιώδεις ιδιότητες του Blockchain
- Η επεξήγηση της έννοιας των λειτουργικών και μη-λειτουργικών απαιτήσεων στα πλαίσια των Αποκεντρωμένων εφαρμογών (dApps).

- Η παρουσίαση των διαφορετικών Blockchain εφαρμογών σαν υποψήφια για την ανάπτυξη Αποκεντρωμένων Εφαρμογών (dApps).
- Η απεικόνιση της ροής των πληροφοριών στο αρχιτεκτονικό επίπεδο των Αποκεντρωμένων Εφαρμογών (dApps).
- Η παρουσίαση της Τεχνολογικής στοιβάδας των Αποκεντρωμένων Εφαρμογών (dApps).
- Η παρουσίαση διαφόρων περιπτώσεων της χρήσης που κτίζονται με βάση τις Αποκεντρωμένες Εφαρμογές (dApps).
- Η επεξήγηση των πιθανών συνεργιών των Αποκεντρωμένων Εφαρμογών με άλλες νέες τεχνολογίες που ανθίζουν.
- Η συζήτηση γύρω από το Νομικό πλαίσιο για τις επιπτώσεις των Αποκεντρωμένων Εφαρμογών (dApps).

Μαθησιακά αποτελέσματα

- Η αξιολόγηση της απαίτησης χρήσης μιας Αποκεντρωμένης Εφαρμογής σε αντίθεση με ένα παραδοσιακό Κεντρικό Μοντέλο
- Η ανάλυση των βασικών χαρακτηριστικών των Αποκεντρωμένων εφαρμογών με τις θεμελιώδεις ιδιότητες των Blockchain εφαρμογών.
- Ο προσδιορισμός και η ανάλυση των λειτουργικών και μη-λειτουργικών απαιτήσεων των Αποκεντρωμένων εφαρμογών
- Η αξιολόγηση της καταλληλόλητας των διαφορετικών Blockchain εφαρμογών για τις Αποκεντρωμένες Εφαρμογές.
- Ο σχεδιασμός των Αρχιτεκτονικών Ροών για τις Αποκεντρωμένες Εφαρμογές
- Ο προσδιορισμός και η ανάλυση των κύριων Τεχνολογικών επιπέδων των Αποκεντρωμένων Εφαρμογών
- Η αναφορά της χρήσης των εφαρμογών σε διαφορετικές περιπτώσεις
- Ο συσχετισμός των Αποκεντρωμένων Εφαρμογών σε άλλες αναδυόμενες τεχνολογίες
- Ο προσδιορισμός απαιτήσεων που ενδέχεται να εγείρουν νομικά ζητήματα

Περίληψη

1. Ανατομία των Αποκεντρωμένων Εφαρμογών
   1.1. Επισκόπηση των Εφαρμογών του Blockchain
   1.2. Παραδείγματα εφαρμογής
   1.3. Παραδείγματα χρήσης
2. Σχέδια σχεδιασμού Αποκεντρωμένων Εφαρμογών (dApp)
   2.1. Μοτίβα αλληλεπίδρασης με τον εξωτερικό κόσμο
   2.2. Πρότυπα διαχείρισης δεδομένων
   2.3. Σχέδια ασφαλείας
   2.4. Διαρθρωτικά σχέδια συμβολαίου
3. Βασικές εφαρμογές των Αποκεντρωμένων Εφαρμογών
   3.1. Προγραμματισμός δημόσιων/ανοιχτής φύσεως Blockchain
   3.2. Προγραμματισμός ιδιωτικού/ πρόσβασης με συναίνεση Blockchain
   3.3. Κύκλος Ζωής των Αποκεντρωμένων Εφαρμογών (dApps)
4. Παραδείγματα των προηγμένων χρήσεων της Τεχνολογίας

Ενότητα μάθησης 8: Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (DAO)

Περιγραφή

Οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (DAO) είναι οργανισμοί που λειτουργούν αυτόνομα και θα μπορούσαν να λάβουν αποκεντρωμένες αποφάσεις μέσω της χρήσης τεχνολογίας, π.χ. Τεχνολογία Blockchain, Directed Acyclic Graphs (DAG), Hashgraph αλγόριθμος κ.λπ. Ένας αποκεντρωμένος αυτόνομος οργανισμός (DAO) είναι συνήθως ένας οργανισμός που εκτελείται μέσω πρωτοκόλλων που κωδικοποιούνται ως διάφοροι τύποι προγραμμάτων υπολογιστών που ονομάζονται Έξυπνα Συμβόλαια.

Οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (DAOs) μερικές φορές αναφέρονται επίσης ως αποκεντρωμένες αυτόνομες εταιρείες (DAC). Οι οικονομικές συναλλαγές και τα αρχεία πρωτοκόλλου του προγράμματος διατηρούνται στο Blockchain ή σε παρόμοιες τεχνολογίες. Αυτοί οι τύποι οργανισμών είναι παρόμοιοι με οποιονδήποτε οργανισμό στον πραγματικό κόσμο, ωστόσο στον ψηφιακό κόσμο οι κανόνες ενός οργανισμού (π.χ. μια εταιρεία) δεν εφαρμόζονται ψηφιακά.

Είναι ψηφιακά και υπάρχουν ήδη από τη φύση τους. Τα DAOs είναι σαν μια κρυπτογραφική δημοκρατία για έναν οργανισμό, όπου κάθε ενδιαφερόμενος μπορεί να ψηφίσει για να προσθέσει νέα πρωτόκολλα, να αλλάξει τα υπάρχοντα πρωτόκολλα ή να συμπεριλάβει και να αποκλείσει ένα μέλος μεταξύ άλλων τύπων δικαιωμάτων.

Η Ενότητα μάθησης 8, θα αναλύσει τα κύρια χαρακτηριστικά των Αποκεντρωμένων Αυτόνομων Οργανισμών (DAOs), καθώς και τα πλεονεκτήματα και τα μειονεκτήματά τους. Ιδιαίτερη προσοχή θα δοθεί στις νομικές, πολιτιστικές και πολιτικές συνέπειες της χρήσης αυτού του ανατρεπτικού παραδείγματος. Μια μελέτη περίπτωσης ενός DAO αναλύεται λεπτομερώς. Τέλος, ένα εργαστήριο ειδικά σχεδιασμένο για τεχνικό κοινό, θα εξηγήσει πώς να εφαρμόσει DAO στην υποδομή Ethereum.

Προαπαιτούμενα

Η ενότητα έχει ως προαπαιτούμενες τις ακόλουθες ενότητες:

- Εισαγωγή στο μάθημα και στον κόσμο των DLTs (LM0)
- Έξυπνα Συμβόλαια (LM5)
- Δικαιώματα απορρήτου και ιδιοκτησίας (LM6)

Στόχοι μαθήματος

- Να εισαγάγει την έννοια του αποκεντρωμένου αυτόνομου οργανισμού (DAO) ως επέκταση ενός dApp.
- *Η π*αρουσίαση των δομών και των μηχανισμών διακυβέρνησης εντός ενός DAO.
- *Να συζητηθούν* τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης ενός DAO για τη διαχείριση ενός οργανισμού.
- *Η π*αρουσίαση ζητημάτων ασφάλειας, ζητημάτων νομικής ευθύνης και κινδύνων DAO.
- *Να συζητηθούν οι* πολιτιστικές και πολιτικές επιπτώσεις των DAO.
- Να αναλύσει σε βάθος μια συγκεκριμένη περίπτωση χρήσης του DAO.

- *Να παρουσιαστούν* πιθανές μελλοντικές εξελίξεις των DAO.
- Για να δείξετε πώς να εφαρμόσετε ένα DAO στο *Blockchain και στο* Ethereum *με την χρήση* Solidity.

Μαθησιακά αποτελέσματα

- Η κατανόηση της βασικής ιδέα των DAOs.
- Η κατανόηση των πλεονεκτημάτων και των μειονεκτημάτων της χρήσης DAO.
- Η αναφορά των νομικών κινδύνων και των κινδύνους ασφαλείας των DAO.
- Η περιγραφή των σημαντικών περιπτωσιολογικών μελετών χρησιμοποιώντας DAO.
- Η εφαρμογή ενός DAO στο Solidity.

Περίληψη

6. Εισαγωγή στους Αποκεντρωμένους Αυτόνομους Οργανισμούς
   1.1. Ορισμός των DAOs
   1.2. Από dApps σε DAO
   1.3. Δομή των DAO
   1.4. Δημοκρατία εντός των DAO
7. Πλεονεκτήματα και μειονεκτήματα
   2.1. Πλεονεκτήματα των DAO
   2.2. Μειονεκτήματα των DAO
   2.3. Προκλήσεις με D AOs
   2.4. Αποτελεσματικότητα των DAO
8. Ασφάλεια, νομική ευθύνη και κίνδυνοι
   8.1. Ασφάλεια των DAO
   8.2. Νομική ευθύνη των DAO
   8.3. Κίνδυνοι που σχετίζονται με DAO)
9. Πολιτιστικές και πολιτικές επιπτώσεις
   9.1. Πολιτιστικές διαφορές και επιπτώσεις των DAO
   9.2. Πολιτικά συστήματα και υλοποιήσεις των DAO
10. Μελέτη περίπτωσης αποκεντρωμένων αυτόνομων οργανισμών (DAO)
    5.1. Εξερεύνηση μιας υπόθεσης DAO
    5.2. Διδάγματα από τη μελέτη περίπτωσης
11. Το μέλλον των DAOs
12. Εργαστήριο: Εφαρμογή DAO στο Solidity