BLOCKCHAIN ΚΑΙ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ: ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΡΟΕΚΤΑΣΕΙΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μπισδούνη Αριστέα (ΑΜ 16140)

Επιβλέπων Καθηγητής: Αναγνωστάκης Αριστείδης

Πρέβεζα - 2019

Πανεπιστήμιο Ιωαννίνων
Τμήμα Λογιστικής και Χρηματοοικονομικής

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΔΙΟΙΚΗΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

BLOCKCHAIN ΚΑΙ «ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ»: ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΡΟΕΚΤΑΣΕΙΣ

Μπισδούνη Αριστέα

Επιβλέπων: Αναγνωστάκης Αριστείδης

Πρέβεζα, 2019

BLOCKCHAIN AND “SMART CONTRACTS”: APPLICATIONS AND EXTENSIONS

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Πρέβεζα, 13/05/2019

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων Καθηγητής[1]

Αριστείδης Αναγνωστάκης

Λέκτορας, Τμήματος Λογιστικής και Χρηματοοικονομικής Πανεπιστημίου Ιωαννίνων

2. Μέλος επιτροπής

Παρασκευή Παππά

Λέκτορας, Τμήματος Λογιστικής και Χρηματοοικονομικής Πανεπιστημίου Ιωαννίνων

3. Μέλος επιτροπής

Ειρήνη Τριάρχη

Λέκτορας, Τμήματος Λογιστικής και Χρηματοοικονομικής Πανεπιστημίου Ιωαννίνων

Ο Προϊστάμενος του Τμήματος

Κωνσταντίνος, Καραμάνης

Αναπληρωτής Καθηγητής, Τμήματος Λογιστικής και Χρηματοοικονομικής Πανεπιστημίου Ιωαννίνων

[1] Η αξιολόγηση της εργασίας πραγματοποιήθηκε αντικαθιστώντας ο κ. Καραμάνης τον κ. Αναγνωστάκη που απουσίαζε λόγω εκπαιδευτικής άδειας.

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα πτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Μπισδούνη, Αριστέα

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της εργασίας μου, κ. Αναγνωστάκη καθώς και τα μέλη του ΔΕΠ Τμήματος Λογιστικής και Χρηματοοικονομικής για την υποστήριξή τους στην ολοκλήρωση των σπουδών μου. Επιπλέον, ευχαριστώ το σύζυγό μου Χρήστο και τα παιδιά μου Κατερίνα, Χριστίνα και Γιώργο για την υπομονή που έδειξαν καθ' όλη τη διάρκεια των σπουδών μου στο Τμήμα.

ΠΕΡΙΛΗΨΗ

Η τεχνολογία blockchain ξεκίνησε να συζητείται με την εμφάνιση του bitcoin. Το bitcoin ως το πλέον επιτυχημένο, μέχρι σήμερα, παράδειγμα κρυπτονομίσματος επιτρέπει την εκτέλεση χρηματικών συναλλαγών μεταξύ αγνώστων χωρίς να υπάρχει κάποια έμπιστη οντότητα η οποία θα μεσολαβήσει έτσι ώστε να εγγυηθεί την εγκυρότητα των συναλλαγών. Η ορθή λειτουργία του bitcoin στηρίζεται σε ένα καθολικό (ledger) στο οποίο καταγράφονται οι συναλλαγές και το οποίο διατηρείται σε πολλά αντίγραφα σε ένα ομότιμο σύστημα. Η δε εισαγωγή νέων συναλλαγών επιβεβαιώνεται μέσω κοινής συναίνεσης των συμμετεχόντων η οποία στηρίζεται στη συλλογική διάθεση υπολογιστικής ισχύος.

Πλέον, αποτελεί κοινή αποδοχή ότι η τεχνολογία blockchain υπερβαίνει την εφαρμογή bitcoin. Στη διαμόρφωση αυτής της άποψης έχουν συμβάλει εκατοντάδες άλλα κρυπτονομίσματα τα οποία κυκλοφορούν αλλά και το Ethereum που εισήγαγε την έννοια της χρήση ενός blockchain συστήματος έτσι ώστε να υποστηριχθεί μια ευρύτερη γκάμα εφαρμογών. Αυτό γίνεται μέσω της χρήσης των έξυπνων συμβολαίων και μπορεί να οδηγήσει έως και στη δημιουργία των λεγόμενων κατανεμημένων αυτόνομων οργανισμών (Decentralized Autonomous Organizations=DAOs). Τα έξυπνα συμβόλαια αποτελούν αυτό-εκτελούμενα συμβόλαια που περιέχουν όρους συμφωνίας ανάμεσα σε αγοραστές και πωλητές απευθείας καταγεγραμμένους σε κώδικα. Οι πιθανές εφαρμογές των έξυπνων συμβολαίων είναι πολλές όπως οι ασφάλειες, οι αγοραπωλησίες γης, η κατοχύρωση πνευματικών δικαιωμάτων, η δημιουργία μητρώων πιστοποιητικών κ.α.

Οι δύο βασικές κατηγορίες blockchain συστημάτων είναι τα blockchain συστήματα που δεν απαιτούν άδειες συμμετοχής και τα blockchain συστήματα με άδειες συμμετοχής. Στην επιστημονική κοινότητα αλλά και στον κόσμο των επιχειρήσεων φαίνεται να υπάρχει σημαντικό ενδιαφέρον όπως καταδεικνύεται από τη δημοσιότητα που έχει αποκτήσει ο όρος blockchain και τη πληθώρα ερευνητικών και άλλων έργων που επικαλούνται τα πλεονεκτήματα του blockchain.

Η παρούσα εργασία εξετάζει τα κρυπτονομίσματα, την τεχνολογία blockchain και τα έξυπνα συμβόλαια. Παρουσιάζει πιθανές εφαρμογές του blockchain σε διάφορους κλάδους. Από την άλλη μεριά αναδεικνύει ελλείψεις και προβλήματα που φαίνεται να υπάρχουν στην εν λόγω τεχνολογία.

Λέξεις-κλειδιά: blockchain, έξυπνα συμβόλαια, κρυπτονομίσματα.

ABSTRACT

Blockchain became a popular topic soon after the emergence of bitcoin. Bitcoin is the most successful example of cryptocurrency, until today. It allows financial transactions among untrusted parties without the need of an authority that should vouch for the legitimacy of them. Bitcoin's sound operation is based on a ledger that keeps all transactions and is shared in many copies among members of a peer to peer system. New transactions are verified through a common consensus algorithm which is based on spending computing power.

It is believed that blockchain transcend its application on bitcoin. The existence of numerous other successful cryptocurrencies seems to support such an opinion. Ethereum introduced the concept of using a blockchain system to support a wider range of applications. This is achieved through smart contracts that can be used in order to capture as computer code various agreements among parties. Furthermore, complex smart contracts can form what is known as Decentralized Autonomous Organizations (DAOs). Smart contract applications are numerous including insurances, real estate, copyrights, certificates etc.

Two major categories of blockchain systems exist: permission-less blockchain and permissioned blockchain. Great interest exists for both and the popularity of the blockchain term keeps rising. Numerous research and other projects embed blockchain in an attempt to acquire benefits that are usually attributed to blockchain

In this work, cryptocurrencies, blockchain and smart contracts are examined. A number of possible blockchain applications are presented. Nevertheless, a critical view is taken and shortcomings of the blockchain technology in its current state are discussed.

Keywords: blockchain, smart contracts, cryptocurrency

Πίνακας περιεχομένων

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ/ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

- ASIC: Application Specific Integrated Circuit
- BTC: Bitcoin
- DAO: Decentralized Autonomous Organizations
- DApp: Decentralized Application
- ECDSA=Elliptic Curve Digital Signing Algorithm
- ETH: Ether
- ICO: Initial Coin Offering
- LTC: Litecoin
- Nonce: Number used once
- P2P: Peer to Peer
- PoS: Proof of Stake
- PoW: Proof of Work
- SHA256: Secure Hash Algorithm 256 bits
- SPV: Simplified Payed Verifications
- ZKP: Zero Knowledge Proof

ΑΠΟΔΟΣΗ ΟΡΩΝ / ΓΛΩΣΣΑΡΙΟ

- **51% επίθεση**: μια 51% επίθεση αναφέρεται σε μια επίθεση σε ένα blockchain σύστημα που οργανώνεται από έναν σύνολο εξορυκτών που διαθέτουν περισσότερο από το 50% της υπολογιστικής ισχύος των εξορυκτών που συμμετέχουν στο σύστημα. Σε αυτή την περίπτωση οι επιτιθέμενοι θα ήταν σε θέση να εμποδίσουν συναλλαγές να επαληθευτούν, να ακυρώσουν συναλλαγές που έχουν ολοκληρωθεί και να πραγματοποιήσουν συναλλαγές στο blockchain προς όφελός τους.
- **Bitcoin**: Το bitcoin είναι ένα κρυπτονόμισμα, και αποτελεί μια μορφή ηλεκτρονικού χρήματος. Είναι ένα αποκεντρωμένο ψηφιακό νόμισμα που δεν εξαρτάται από μια κεντρική τράπεζα ή κάποιο μεμονωμένο διαχειριστή και το οποίο μπορεί να αποσταλεί από έναν χρήστη του ομότιμου bitcoin δικτύου σε έναν άλλο χωρίς τη χρήση μεσαζόντων.
- **Blockchain**: Το Blockchain είναι ένα κατανεμημένο καθολικό (distributed ledger), δημόσιο ή ιδιωτικό, στο οποίο συναλλαγές ή δεδομένα συνδέονται μεταξύ τους σε συνδεδεμένα μπλοκ δεδομένων καθιστώντας τα πρακτικά αμετάβλητα και αδιαμφισβήτητα από όλους τους κατανεμημένους κόμβους στους οποίους έχει γίνει η ενημέρωση του καταλόγου.
- **Decentralized Autonomous Organization (DAO)**:
- **Ethereum**: Το Ethereum είναι μια blockchain πλατφόρμα που εκτελεί εξ αποστάσεως κώδικα σε ένα κατανεμημένο υπολογιστικό σύστημα που λέγεται Ethereum Virtual Machine.
- **Full nodes**: Κόμβοι που περιέχουν το πλήρες blockchain.
- **Genesis block**: Το πρώτο μπλοκ σε ένα blockchain.
- **Initial Coin Offering (ICO)**: Μηχανισμός χρηματοδότησης για επιχειρηματικές ιδέες οι οποίες στηρίζονται στο blockchain. Δημιουργείται ένα νέο νόμισμα που απαιτείται έτσι ώστε να επιτρέπεται η χρήση της εφαρμογής μέσω της οποίας θα υλοποιείται η επιχειρηματική ιδέα. Ένας αριθμός αυτών των νομισμάτων διατίθενται προς πώληση πριν την εκκίνηση της εφαρμογής έτσι ώστε οποιοσδήποτε ενδιαφερόμενος να μπορεί να τα αποκτήσει.
- **Light nodes**: Κόμβοι του δικτύου blockchain που «κατεβάζουν» μόνο τις κεφαλές των μπλοκς και για αυτό τον λόγο έχουν χαμηλότερες απαιτήσεις εκτέλεσης. Χρησιμοποιώντας μια μέθοδο που ονομάζεται Simplified Payment Verifications (SPV), ένας light node μπορεί να υποβάλει ερώτημα σε έναν full node για την επαλήθευση μιας συναλλαγής. Παραδείγματα light nodes αποτελούν τα κρυπτογραφικά πορτοφόλια.
- **Merkle tree**: Δεντρική δομή αποθήκευσης συναλλαγών που διασφαλίζει ότι σε περίπτωση αλλαγής των στοιχείων μιας συναλλαγής αυτό γίνεται ανιχνεύσιμο εξετάζοντας την τιμή της ρίζας του δένδρου (Merkle root) σε σχέση με την προηγούμενη τιμή που είχε. Το Merkle root αποθηκεύεται στην κεφαλή του μπλοκ και τα στοιχεία των συναλλαγών αποθηκεύονται στο μπλοκ ως ένα Merkle tree.
- **Miners**: Οι miners (εξορύκτες) προσπαθούν να προσαρτήσουν νέα μπλοκ στο blockchain. Όταν ένας miner επιτύχει να προσαρτήσει ένα νέο μπλοκ τότε λαμβάνει τόσο την αμοιβή εξόρυξης, όσο και τα κόστη συναλλαγών. Αυτός ο τρόπος λειτουργίας δίνει κίνητρο στους miners έτσι ώστε να επικυρώνουν νέες συναλλαγές σε συνεχή βάση και με αυτό τον τρόπο να υποστηρίζουν τη λειτουργία του blockchain.
- **Nonce**: Ένας αριθμός που θα πρέπει να «μαντευθεί» (μέσω πολλών πειραματισμών τύπου trial and error) και ο οποίος συνδυαζόμενος με τα υπόλοιπα στοιχεία ενός μπλοκ και το hash value του προηγούμενου μπλοκ θα οδηγήσει στην παραγωγή ενός

νέου hash value που θα καλύπτει το απαιτούμενο επίπεδο δυσκολίας (αριθμός από μηδενικά στην αρχή του hash value) όπως ορίζεται δυναμικά από το δίκτυο.

- **Permissioned blockchain**: Είδος blockchain στο οποίο οι συμμετέχοντες είναι γνωστοί και έχουν λάβει άδεια συμμετοχής στο σύστημα. Υπάρχει κάποιος βαθμός εμπιστοσύνης ανάμεσα στους συμμετέχοντες. Αναφέρεται και ως ιδιωτικό blockchain.
- **Permission-less blockchain**: Είδος blockchain στο οποίο μπορεί να συμμετέχει οποιοσδήποτε και το οποίο επιβεβαιώνει τις συναλλαγές με βάση τη συναίνεση που δημιουργείται από τα μέλη του που πρέπει να αφιερώσουν υπολογιστική ισχύ για την επαλήθευση των συναλλαγών. Αναφέρεται και ως δημόσιο blockchain.
- **Proof of Stake (PoS)**: Μια μορφή αλγορίθμου μέσω του οποίου ένα blockchain σύστημα στοχεύει στην επίτευξη κατανεμημένης κοινής συναίνεσης. Σε ένα PoS σύστημα ο δημιουργός του επόμενου μπλοκ επιλέγεται με τυχαίο τρόπο βάσει αξίας που έχει αποκτήσει ή βάσει χρόνου συμμετοχής στο σύστημα.
- **Proof of Work (PoW)**: Μια μορφή αλγορίθμου μέσω του οποίου ένα blockchain σύστημα στοχεύει στην επίτευξη κατανεμημένης κοινής συναίνεσης. Σε ένα PoW η προσπάθεια εστιάζει στη διαδικασία εύρεσης ενός κατάλληλου nonce. Η βασική ιδέα είναι ότι το nonce είναι δύσκολο να βρεθεί αλλά εύκολο να επαληθευτεί.
- **Smart contract**: Τα smart contracts (έξυπνα συμβόλαια) είναι αυτό-εκτελούμενα συμβόλαια που περιέχουν τους όρους συμφωνίας ανάμεσα στον αγοραστή και στον πωλητή απευθείας καταγεγραμμένους ως γραμμές κώδικα. Τα έξυπνα συμβόλαια καθιστούν τις συναλλαγές ανιχνεύσιμες, διαφανείς και μη αντιστρέψιμες από τη στιγμή που έχουν πραγματοποιηθεί και μετά.

1 Εισαγωγή

Το blockchain αποτελεί έναν όρο που είναι εξαιρετικά δημοφιλής σήμερα. Η κατανόηση του τι είναι το blockchain παρουσιάζει δυσκολίες αλλά οι πιθανές εφαρμογές της νέας αυτής τεχνολογίας είναι τόσο πολλές που έχουν δημιουργήσει ισχυρό ενδιαφέρον από διάφορους κλάδους όπως οι τράπεζες, οι ασφάλειες, η ηλεκτρονική διακυβέρνηση, ο χώρος της υγείας κ.α. Ειδικοί εκτιμούν ότι έχει τις προδιαγραφές έτσι ώστε να προκαλέσει ανατάραξη (disruption) στην καθημερινότητα πολιτών και επιχειρήσεων ανάλογη με αυτή που έχει επιφέρει το διαδίκτυο από τη δεκαετία του 1990 και μετά [1]. Οι αλλαγές που ενδέχεται να επιφέρει εστιάζονται στην αύξηση της αποδοτικότητας των συναλλαγών για οτιδήποτε συναλλάσσεται με την ταυτόχρονη διασφάλιση της εγκυρότητας των συναλλαγών.

Το blockchain αποτελεί ένα ψηφιακό και αποκεντρωμένο καθολικό (digital decentralized ledger) στο οποίο καταγράφονται με ασφάλεια πληροφορίες που μπορούν να προσπελάσουν οι συμμετέχοντες σε αυτό. Βάσει σχεδιασμού, οι πληροφορίες που καταγράφονται στο blockchain δεν μπορούν να αλλάξουν (immutable) από τη στιγμή που έχουν εισαχθεί σε αυτό. Μια συναλλαγή μπορεί να «ακυρωθεί», μόνο μέσω μιας άλλης συναλλαγής και σε αυτή την περίπτωση και οι δύο συναλλαγές παραμένουν ορατές στο blockchain. Αν και αυτό αρχικά φαίνεται ως περιορισμός, στην πράξη λειτουργεί ως πλεονέκτημα καθώς προσδίδει εμπιστοσύνη και εγκυρότητα στα στοιχεία που εν τέλει εμπεριέχονται στο blockchain [2].

Οι πληροφορίες που καταγράφονται στο blockchain μπορεί να αφορούν οτιδήποτε. Συνηθισμένες περιπτώσεις αποτελούν η καταγραφή ιδιοκτησίας (με υλική υπόσταση όπως για παράδειγμα ένα σπίτι ή άυλη όπως για παράδειγμα πνευματικά δικαιώματα, πατέντες κ.α.) και η καταγραφή συναλλαγών.

Το blockchain είναι συνυφασμένο στην αντίληψη πολλών με τα κρυπτονομίσματα και

ιδιαίτερα με το bitcoin. Πράγματι, τοαξίζει να παρακολουθηθούν για το έτος 2018 blockchain αποτελεί την υποδομή πάνω στην[3]. Ιδρύθηκε, καθώς εντοπίστηκαν οποία λειτουργεί το bitcoin αλλά μπορεί ναπροβλήματα στον τομέα της αγοράς αποτελέσει υποδομή και για άλλες εφαρμογέςμεταχειρισμένων αυτοκινήτων αλλά και ανεξάρτητα από τον κόσμο τωνγενικότερα της αυτοκίνησης που μπορούν να κρυπτονομισμάτων. Συνεπώς, το bitcoin είναιεπιλυθούν με τη χρήση της τεχνολογίας. Τα μόνο μια (και ιστορικά η πρώτη) εφαρμογήπροβλήματα αυτά, όπως αναφέρει η ίδια η του blockchain. εταιρεία στην ιστοσελίδα της, είναι:

Οι μεγάλες εταιρείες τεχνολογίας δεν έχουν μείνει ασυγκίνητες από τη νέα αυτή τεχνολογία. Η Microsoft προσφέρει εργαλεία κατασκευής εφαρμογών blockchain στην υπολογιστική υποδομή νέφους που διαθέτει, το Azure cloud. Η IBM, η Intel και άλλες εταιρείες συνεργάζονται στην δημιουργία του Hyperledger που αποτελεί μια τεχνολογία blockchain με έμφαση σε επιχειρηματικές εφαρμογές. Στο ίδιο μήκος κύματος βρίσκονται και οι τράπεζες που προσπαθούν να στρέψουν την blockchain τεχνολογία προς όφελός τους.

Η παρούσα πτυχιακή εξετάζει το blockchain, τα έξυπνα συμβόλαια και τα κρυπτονομίσματα καθώς και εφαρμογές του blockchain σε διάφορα πεδία.

- Το ιστορικό των οχημάτων όπως καταγράφεται συχνά είτε δεν είναι ενημερωμένο είτε είναι λανθασμένο είτε περιέχει εσκεμμένα εσφαλμένες πληροφορίες. Η δε πρόσβαση σε αυτό είναι ακριβή.
- Οι αγοραστές μεταχειρισμένων οχημάτων δεν μπορούν να είναι σίγουροι για την πραγματική αξία της αγοράς τους.
- Δεν υπάρχει κίνητρο για τους καταναλωτές και τις επιχειρήσεις έτσι ώστε να κοινοποιήσουν πληροφορίες σχετικά με τα οχήματα τους.
- Τα δεδομένα των οχημάτων δεν είναι δημόσια διαθέσιμα αλλά η πληροφορία βρίσκεται διάσπαρτη ανάμεσα σε κατασκευαστές, σε τοπικές αντιπροσωπείες οχημάτων, σε συνεργεία οχημάτων και σε άλλους.

1.1 Παράδειγμα εφαρμογής του blockchain

Ως παράδειγμα του πως η τεχνολογία blockchain, ενδεχόμενα, μπορεί να μετασχηματίσει έναν υπάρχοντα επαγγελματικό χώρο, παρουσιάζεται η επιχειρηματική ιδέα VINchain[2] που αφορά την αγορά μεταχειρισμένων αυτοκινήτων στις ΗΠΑ. Θα πρέπει να σημειωθεί ότι το συγκεκριμένο παράδειγμα δεν παρουσιάζεται κατ' ανάγκη ως «επιτυχημένη περίπτωση χρήσης του blockchain» καθώς το όλο εγχείρημα δεν έχει ακόμα ολοκληρωθεί και συνεπώς δεν μπορούν να ληφθούν ασφαλή συμπεράσματα για την επιτυχία ή μη του όλου εγχειρήματος.

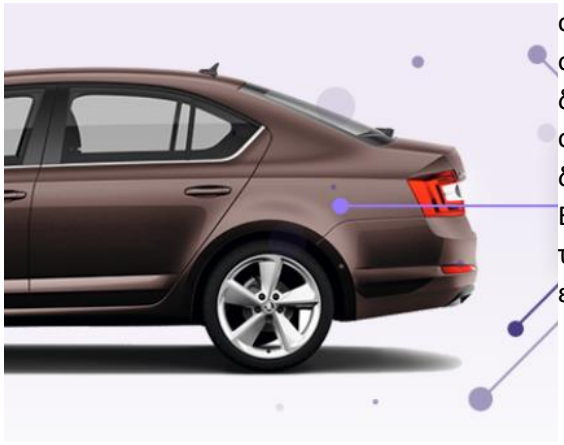
Η εταιρεία VINChain συμπεριλήφθηκε από το Enterpreneur Europe[3] στις 14 εταιρείες που

Ο στόχος της VINChain είναι να εξαλείψει την ασυμμετρία πληροφόρησης ανάμεσα στον πωλητή και στον αγοραστή μεταχειρισμένων οχημάτων διατηρώντας στο blockchain το ιστορικό των οχημάτων. Για κάθε όχημα εισάγεται η ιδέα του VIN (Vehicule Identification Number) που λειτουργεί ως αριθμός διαβατηρίου για οχήματα και ο οποίος καταγράφει αριθμητικά και με ακρίβεια το πλήρες ιστορικό του κάθε οχήματος που διαθέτει VIN. Αυτό επιτυγχάνεται με μια συσκευή που πρέπει να εγκατασταθεί σε κάθε αυτοκίνητο και η οποία συλλέγει πληροφορίες από το ίδιο το όχημα και μια εφαρμογή που παρουσιάζει αυτά τα στοιχεία και τα αποθηκεύει στο blockchain. Ο συνδυασμός των δεδομένων που συλλέγονται

[2] https://vinchain.io/

[3] https://www.entrepreneur.com/

από το ίδιο το όχημα με δεδομένα από άλλεςνα εντοπιστούν και για τους ασφαλιστικούς βάσεις δεδομένων και η αποθήκευση τηςοργανισμούς και για άλλες συνεργαζόμενες σχετικής πληροφορίας στο blockchainεπιχειρήσεις.
διασφαλίζει ότι τα δεδομένα δεν μπορούν να αλλαχθούν κακόβουλα (π.χ. αλλαγή αριθμού χιλιομέτρων που έχει διανύσει το όχημα).



Εικόνα 1. Η συσκευή και το App της εταιρείας VINchain

Η επιχείρηση VINChain προσφέρει επιπλέον του ακριβούς ιστορικού οχήματος, τη δυνατότητα στους πελάτες της να αποκτήσουν VIM tokens (σύστημα ανταμοιβών) αλλά και να παρακολουθούν οι ίδιοι συνεχώς το όχημά τους και να δέχονται χρήσιμες πληροφορίες σχετικά με αυτό. Ανταμοιβές λαμβάνουν τόσο οι οδηγοί οχημάτων που εγκαθιστούν τη συσκευή της εταιρείας στο όχημά τους όσο και επιχειρήσεις όπως κατασκευαστές, αντιπροσωπείες, συνεργεία, ασφαλιστικές εταιρείες και άλλες. Η ανταμοιβή μπορεί να αφορά εκπτώσεις, ανταλλαγή των VIM tokens με δολάρια ή ευρώ, αναλυτικές αναφορές ιστορικού οχήματος και άλλες. Τα δε πλεονεκτήματα ενός «συνδεδεμένου οχήματος» είναι η συνεχής παρακολούθηση του οχήματος (π.χ. δυνατότητα συναγερμού όταν το όχημα βρεθεί εκτός συγκεκριμένων γεωγραφικών περιοχών), ανάλυση οδήγησης (π.χ. ασφαλέστερη και οικονομικότερη οδήγηση), καταγραφή συμβάντων με χρονικές σφραγίδες (π.χ. συγκρούσεις, επιδιορθώσεις). Οι αντιπροσωπείες μπορούν να οργανώσουν καλύτερα το χρόνο των services και των επιδιορθώσεων και να πετύχουν χαμηλότερο χρόνο αναμονής και υψηλότερη ικανοποίηση πελατών. Ανάλογα πλεονεκτήματα μπορούν

Στην περίπτωση της VINChain αλλά και γενικότερα το blockchain χρησιμοποιείται έτσι ώστε να ενισχύσει την εμπιστοσύνη ανάμεσα στα μέλη ενός επιχειρηματικού δικτύου. Οι συναλλαγές ομαδοποιούνται και παρέχεται διασφάλιση για κάθε ομάδα συναλλαγών ότι οποιαδήποτε απόπειρα αλλαγής των δεδομένων θα γίνεται άμεσα αντιληπτή. Ειδικότερα, οι ιδιότητες του blockchain που του επιτρέπουν να παρέχει τη ζητούμενη εμπιστοσύνη είναι οι ακόλουθες [4]:

1. **Κατανεμημένο**: Το blockchain είναι διαμοιρασμένο στους συμμετέχοντες, και διατηρείται σε σχεδόν πραγματικό χρόνο ενημερωμένο με τις νεότερες συναλλαγές. Δεν βρίσκεται υπό την αποκλειστική ιδιοκτησία ενός οργανισμού και η συνέχεια της ύπαρξής του δεν εξαρτάται από κάποια μεμονωμένη οντότητα.
2. **Ασφαλές**: Η ύπαρξη δικαιωμάτων πρόσβασης και κρυπτογραφίας αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση. Τόσο η ταυτότητα, όσο και τα στοιχεία των συναλλαγών μπορούν να αποκρυφθούν.
3. **Διαφανές**: Οι συμμετέχοντες σε μια συναλλαγή έχουν πρόσβαση στις ίδιες εγγραφές και μπορούν να επιβεβαιώσουν τις ταυτότητες των άλλων μελών χωρίς να εμπλέκονται τρίτα μέρη (third party) ως ενδιάμεσοι. Οι συναλλαγές έχουν χρονικές σφραγίδες και μπορούν να επαληθευθούν σε πραγματικό χρόνο.
4. **Κοινή συναίνεση**: Η εγκυρότητα των συναλλαγών αποφασίζεται με κοινή συναίνεση των μελών του δικτύου. Ανάλογα με τις απαιτήσεις που έχουν οριστεί καθορίζονται και οι προϋποθέσεις σύμφωνα με τις οποίες οριστικοποιούνται οι συναλλαγές.
5. **Ευέλικτο**: Στο ίδιο το blockchain μπορούν να ενσωματωθούν

επιχειρηματικοί κανόνες και έξυπνα συμβόλαια (που εκτελούνται αυτόματα όταν ικανοποιηθούν κάποιες προϋποθέσεις). Με αυτό τον τρόπο τα επιχειρηματικά δίκτυα μπορούν να εξελίσσονται και να υποστηρίζουν νέες δυνατότητες εφόσον αυτό απαιτηθεί.

2 Βασικές έννοιες

2.1 Κατανεμημένα Συστήματα

Υπάρχουν δύο βασικά είδη συστημάτων, τα συγκεντρωτικά (centralized) και τα κατανεμημένα (distributed). Στα συγκεντρωτικά συστήματα, που είναι γνωστά και ως συστήματα πελάτη-εξυπηρετητή (client-server), υπάρχει ένα τμήμα του συστήματος στο οποίο συνδέονται τα υπόλοιπα και από το οποίο εξαρτάται η λειτουργία του συστήματος στο σύνολό του. Από την άλλη μεριά στα κατανεμημένα συστήματα τα επιμέρους τμήματα του συστήματος συνδέονται χωρίς να υπάρχει τμήμα που να εξυπηρετεί ή να συντονίζει τα άλλα τμήματα και από το οποίο να εξαρτάται η συνολική λειτουργία του συστήματος.

Σε ότι αφορά τα συστήματα λογισμικού, τα κύρια πλεονεκτήματα των κατανεμημένων συστημάτων έναντι των κεντρικών είναι η υψηλότερη υπολογιστική ισχύς, το μειωμένο κόστος, η υψηλότερη διαθεσιμότητα – αξιοπιστία και η μεγαλύτερη δυνατότητα κλιμάκωσης. Ωστόσο, τα κατανεμημένα συστήματα έχουν και μειονεκτήματα με σημαντικότερα τη μεγαλύτερη πολυπλοκότητα, τις επιβαρύνσεις συντονισμού και επικοινωνίας που δημιουργούνται καθώς και θέματα ασφάλειας τα οποία θα πρέπει να αντιμετωπιστούν έτσι ώστε να λειτουργήσουν με αποδεκτό τρόπο.

Το blockchain μπορεί να θεωρηθεί ως ένας μηχανισμός για την επίτευξη ακεραιότητας σε κατανεμημένα συστήματα λογισμικού. Η τεχνολογία blockchain μπορεί να αντικαταστήσει τον ρόλο που αυτή τι στιγμή έχουν οι θεωρούμενες ως έμπιστες οντότητες (π.χ. τράπεζες, ασφαλιστικοί οργανισμοί, κυβερνητικές υπηρεσίες, κ.α.) σε κεντρικά συστήματα μετασχηματίζοντας τα σε αποδοτικότερα κατανεμημένα συστήματα.

2.2 Ομότιμα κατανεμημένα συστήματα

Τα ομότιμα (P2P = peer to peer) κατανεμημένα συστήματα είναι μια ειδική κατηγορία κατανεμημένων συστημάτων που αποτελούνται από επιμέρους υπολογιστές που διαθέτουν κάποιους από τους υπολογιστικούς τους πόρους απευθείας σε όλα τα άλλα μέλη του δικτύου. Όπως δηλώνει και το όνομά τους τα συστήματα αυτά είναι ομότιμα, δηλαδή οι επιμέρους υπολογιστές που συχνά αναφέρονται και ως κόμβοι λειτουργούν ταυτόχρονα ως πάροχοι αλλά και καταναλωτές πόρων στο δίκτυο.

Θα πρέπει να σημειωθεί ότι υπάρχουν πολλές παραλλαγές αρχιτεκτονικής ομότιμων συστημάτων. Για παράδειγμα υπάρχουν τα ομότιμα συστήματα με κεντρικό έλεγχο στα οποία κάποιοι κόμβοι διατηρούν ρόλους που διευκολύνουν και καθιστούν αποδοτικότερη τη λειτουργία του συστήματος. Από την άλλη μεριά σε ένας αμιγές ομότιμο σύστημα απουσιάζει πλήρως η έννοια του κεντρικού συντονισμού και ελέγχου.

Ως προκλήσεις στην υιοθέτηση των ομότιμων συστημάτων μπορούν να αναφερθούν: η ασύμμετρη ταχύτητα ανεβάσματος και κατεβάσματος για τους χρήστες του διαδικτύου όπως προσφέρεται από τους παρόχους διαδικτύου σήμερα, η ασφάλεια στη διάθεση του περιεχομένου που προσφέρεται και η διασφάλιση ότι τα απαιτούμενα δικαιώματα διάθεσης της πληροφορίας υφίστανται.

2.2.1 Η περίπτωση του Naspter

Ένα από τα πρώτα ομότιμα κατανεμημένα συστήματα ήταν το Napster[4] το οποίο λειτούργησε για πρώτη φορά το 1999, έφτασε να έχει 80 εκατομμύρια χρήστες και εξαγοράστηκε το 2002 έναντι 5.3 δισεκατομμυρίων δολαρίων από την εταιρεία Roxio. Η λειτουργία του Napster ανάγκασε τη μουσική βιομηχανία να αλλάξει εκ βάθρων.

[4] https://www.lifewire.com/history-of-napster-2438592

Επρόκειτο για ένα ομότιμο κατανεμημένο σύστημα το οποίο εξάλειφε πλήρως τους μεσάζοντες στη διάθεση μουσικής. Αυτό έγινε εφικτό διότι η μουσική αφενός δεν έχει υλική υπόσταση (μπορεί να ψηφιοποιηθεί πλήρως) και αφετέρου η αντιγραφή και μεταφορά της έχει εξαιρετικά χαμηλό κόστος.

Το Napster έδειξε με εμφατικό τρόπο ότι οποιοδήποτε βιομηχανία λειτουργεί ως μεσάζοντας ανάμεσα σε παραγωγούς προϊόντων που δεν έχουν υλική υπόσταση και πελατών για αυτά τα προϊόντα είναι ευάλωτη και μπορεί να αντικατασταθεί από κάποιο ομότιμο σύστημα. Το παγκόσμιο χρηματοοικονομικό σύστημα είναι μια τέτοια περίπτωση καθώς ένα μικρό μόνο ποσοστό των χρημάτων υπάρχουν σε φυσική μορφή νομισμάτων και χαρτονομισμάτων. Για παράδειγμα η μεταφορά χρημάτων από έναν τραπεζικό λογαριασμό σε έναν άλλο τραπεζικό λογαριασμό σε άλλη χώρα μπορεί να απαιτεί την εμπλοκή ακόμα και 5 μεσαζόντων έτσι ώστε να ολοκληρωθεί. Κάθε μεσάζοντας επιβάλλει καθυστερήσεις και χρεώσεις. Ομοίως, υπηρεσίες όπως η παροχή πιστοποιητικών γέννησης, επιβεβαίωσης ιδιοκτησίας, διπλωμάτων οδήγησης, πτυχίων κ.α. καταγράφουν και παρέχουν ότι τους ζητηθεί σε ψηφιακή μορφή λειτουργώντας ως μεσάζοντες. Συνεπώς και αυτές «κινδυνεύουν» να αντικατασταθούν από αποδοτικότερα κατανεμημένα συστήματα χωρίς μεσάζοντες.

Το Napster αποτέλεσε ένα ομότιμο σύστημα με στοιχεία κεντρικού ελέγχου το οποίο άλλαξε τη μουσική βιομηχανία. Η τεχνολογία blockchain στοχεύει κυρίως σε αμιγή ομότιμα συστήματα και ενδέχεται να αλλάξει την καθημερινότητα πολιτών και επιχειρήσεων. Φιλοδοξεί να αποτελέσει το μηχανισμό μέσω του οποίου θα παρέχεται η ζητούμενη ακεραιότητα αφαιρώντας τους παραδοσιακούς μεσάζοντες που τη διασφάλιζαν μέχρι σήμερα.

2.3 Το πρόβλημα των Βυζαντινών Στρατηγών

Ενα αμιγές ομότιμο κατανεμημένο σύστημα θα πρέπει να είναι σε θέση να αντιμετωπίσει καταστάσεις που σχετίζονται με τεχνικά προβλήματα (στους κόμβους των χρηστών και στο δίκτυο) καθώς και προβλήματα που δημιουργεί η συμπεριφορά κακόβουλων χρηστών. Η δεύτερη απειλή φαίνεται να είναι σημαντικότερη καθώς μπορεί να οδηγήσει σε αποχώρηση των χρηστών από το σύστημα και στην παύση λειτουργίας του συστήματος. Συνεπώς, ζητείται η επίλυση του προβλήματος της διατήρησης της ακεραιότητας σε ένα αμιγές ομότιμο κατανεμημένο σύστημα που αποτελείται από έναν άγνωστο αριθμό χρηστών που δεν γνωρίζουμε εάν είναι αξιόπιστοι και μη κακόβουλοι. Το πρόβλημα αυτό είναι γνωστό στην επιστήμη των υπολογιστών με το όνομα «πρόβλημα Βυζαντινών στρατηγών» [5].

Το σενάριο που περιγράφει το πρόβλημα αφορά δύο αυτοκρατορίες που ο στρατός της μιας αυτοκρατορίας βρίσκεται εντός των τειχών μιας πόλης ενώ τα στρατεύματα της δεύτερης αυτοκρατορίας έχουν περικυκλώσει την πόλη και ελέγχονται από στρατηγούς που περιμένουν να επιτεθούν. Για να μπορέσουν να καταλάβουν την πόλη οι στρατηγοί θα πρέπει να επιτεθούν την ίδια χρονική στιγμή και όλοι μαζί, αλλιώς θα χάσουν τη μάχη και τον πόλεμο. Ο μόνος τρόπος με τον οποίο μπορούν να επικοινωνήσουν και να συντονίσουν την επίθεσή τους είναι μέσω κρυφών αγγελιαφόρων που θα περάσουν μέσα από την πόλη και θα μεταδώσουν μηνύματα στους άλλους στρατηγούς. Το πρόβλημα είναι ότι υπάρχει η πιθανότητα κάποιοι από τους αγγελιαφόρους να συλληφθούν να αποκρυπτογραφηθούν τα μηνύματα που μεταφέρουν και να σταλθούν παραποιημένα στους αποδέκτες. Θεωρώντας ότι οι στρατηγοί εκτός των τειχών έχουν σημαντικά περισσότερους «μαθηματικούς ικανούς να κρυπτογραφούν και να αποκρυπτογραφούν μηνύματα» (υπολογιστική ισχύ) από ότι η αυτοκρατορία

εντός των τειχών αυτό σημαίνει ότι τα μηνύματα μπορούν να κρυπτογραφούνται μετά και να κρυπτογραφηθούν εκ νέου στον απαιτούμενο χρόνο είναι σχετικά αμελητέα.

Στα πλαίσια του blockchain ο όρος «Βυζαντινή ανοχή σφάλματος» σημαίνει ότι το blockchain θεωρείται ως ασφαλές όταν οι κακόβουλοι χρήστες έχουν λιγότερη υπολογιστική ισχύ στη διάθεσή τους από ότι οι υπόλοιποι χρήστες και το γεγονός αυτό καθιστά το blockchain ασφαλές για τη μετάδοση έγκυρων πληροφοριών[5].

2.4 Τι είναι το blockchain;

Το blockchain αποτελεί μια νέα τεχνολογία κατανεμημένης βάσης δεδομένων. Η βασική διαφορά σε σχέση με άλλες τεχνολογίες κατανεμημένων βάσεων δεδομένων είναι ότι ο έλεγχος του blockchain ασκείται από μια ομάδα συμμετεχόντων και όχι από μια κεντρική οντότητα.

Είναι σύνηθες το blockchain να περιγράφεται ως ένα κατανεμημένο καθολικό (distributed ledger) που λειτουργεί πάνω από ένα ομότιμο δίκτυο (peer-to-peer network) διατηρώντας αμετάβλητες (immutable) εγγραφές έτσι ώστε να αντιστέκεται σε ενέργειες κακόβουλων χρηστών. Ο όρος καθολικό αναφέρεται σε ένα σύνολο εγγραφών που περιγράφουν για κάθε περιουσιακό στοιχείο σε ποιον ανήκει καθώς και ποιες συναλλαγές έχουν πραγματοποιηθεί και μεταβίβασαν την κυριότητά του από ένα δικαιούχο σε έναν άλλο.

Ένα blockchain αποτελείται από δεδομένα οργανωμένα σε μονάδες που ονομάζονται blocks. Τα blocks συνδέονται μεταξύ τους σχηματίζοντας μια αλυσίδα. Η αφαίρεση ή η τροποποίηση ενός ενδιάμεσου μπλοκ της αλυσίδας καθιστά τα μπλοκ που ακολουθούν άκυρα. Συνεπώς πρόκειται για μια δομή στην οποία μπορούν μόνο να προστίθενται δεδομένα και στην οποία είναι πρακτικά αδύνατο να πραγματοποιηθεί αλλαγή σε δεδομένα που προστέθηκαν στο παρελθόν. Στο blockchain καταγράφονται πληροφορίες που καταγράφουν το ποιος έχει την ιδιοκτησία συγκεκριμένων πόρων. Παράλληλα διασφαλίζεται ότι μόνο ο πραγματικός ιδιοκτήτης ενός πόρου μπορεί να τον μεταβιβάσει σε κάποιον άλλο.

Υπάρχουν δύο βασικοί τύποι blockchains: τα δημόσια (public ή permission-less) blockchains, και τα ιδιωτικά (private ή permissioned) blockchains. Στα δημόσια blockchains χρησιμοποιείται ένα ειδικό νόμισμα (token) για τη διασφάλιση της λειτουργίας τους και είναι ανοικτά σε οποιονδήποτε επιθυμεί να συμμετάσχει χωρίς να αποκαλύπτει την πραγματική του ταυτότητα. Από την άλλη μεριά, στην περίπτωση των ιδιωτικών blockchains πρέπει να υφίσταται κάποιος μηχανισμός ταυτοποίησης των χρηστών που συμμετέχουν. Συνεπώς, τα μέλη ενός ιδιωτικού blockchain θεωρούνται έμπιστα. Για παράδειγμα το HyperLedger είναι ένα έργο ανοικτού κώδικα και επιτρέπει σε διάφορες επιχειρήσεις να δημιουργήσουν ιδιωτικά blockchains έτσι ώστε να επιτύχουν τους στόχους τους. Σε αυτή την περίπτωση και καθώς οι συμμετέχοντες είναι ταυτοποιημένοι, απασχολούν λιγότερο θέματα όπως η διατήρηση της ανωνυμίας και η αντιμετώπιση κακόβουλης συμπεριφοράς. Άρα, ανάλογα με τον τύπο του blockchain δίνεται έμφαση σε διαφορετικές θέματα:

- Στα δημόσια δίκτυα, όπως το Bitcoin, δίνεται έμφαση στη διαφάνεια των συναλλαγών έτσι ώστε οποιοσδήποτε να έχει πρόσβαση σε ότι καταγράφεται ενώ παράλληλα διασφαλίζεται ότι οι ιδιοκτήτες των λογαριασμών είναι ανώνυμοι.
- Στα ιδιωτικά δίκτυα, όπως αυτά που μπορούν να κατασκευαστούν με το

[5] https://medium.com/coinmonks/byzantine-fault-tolerance-in-a-nutshell-bc7762ffb996

HyperLedger, οι συμμετέχοντες είναι γνωστοί και η έμφαση δίνεται στην αποδοτικότητα των ενημερώσεων των συναλλαγών.

Οι πληροφορίες που καταγράφονται στο blockchain μπορεί να αφορούν οικονομικές συναλλαγές καθώς και οποιαδήποτε άλλη πληροφορία για την οποία υπάρχει λόγος καταγραφής. Η απόφαση για το τι καταγράφεται λαμβάνεται μέσω συναίνεσης (consensus) στην οποία οδηγούνται τα συμμετέχοντα μέλη. Στην περίπτωση των δημόσιων blockchains αυτό συμβαίνει δίνοντας κίνητρα έτσι ώστε να ενθαρρύνεται η ορθή (ζητούμενη) συμπεριφορά και να επιβάλλονται ποινές σε όποιον προσπαθεί να αλλάξει προς όφελός του τα καταγεγραμμένα δεδομένα.

2.5 Εφαρμογές του blockchain

Το blockchain μπορεί να θεωρηθεί ως ένα επιπλέον επίπεδο του διαδικτύου το οποίο παρέχει εμπιστοσύνη. Η μονιμότητα των δεδομένων που καταγράφονται σε αυτό δίνει τη δυνατότητα της διατήρησης της πλήρους πληροφορίας που έχει καταγραφεί. Οτιδήποτε δεν έχει ψηφιοποιηθεί ως διαδικασία μέχρι σήμερα και γίνεται με συμμετοχή μεσαζόντων που θεωρούνται αξιόπιστοι (π.χ. μεταφορά χρηματικών ποσών, αλλαγή ιδιοκτησίας σε τίτλους γης κ.α.) μπορεί με τη χρήση του blockchain να πραγματοποιείται στιγμιαία.

Το δίκτυο του bitcoin ήταν εκείνο στο οποίο για πρώτη φορά παρουσιάστηκε η τεχνολογία blockchain. Περαιτέρω ώθηση έδωσε το δίκτυο Ethereum καθώς ενσωμάτωσε στο blockchain του μια ειδική γλώσσα προγραμματισμού με την οποία μπορούν να γράφονται τα λεγόμενα έξυπνα συμβόλαια ενώ εισήγαγε και άλλες καινοτομίες όπως το Ether και τους DAOs (Decentralized Autonomous Organizations). Το Ether είναι το κρυπτονόμισμα του Ethereum και DAO είναι ένας νέος τρόπος οργάνωσης και ενσωμάτωσης εταιρειών πάνω στο δίκτυο του Ethereum.

2.6 Κοινή συναίνεση (consensus)

Η επιβολή των απαιτούμενων κανόνων στους κόμβους του δικτύου που είναι επιφορτισμένοι με την επαλήθευση των στοιχείων που πρόκειται να καταγραφούν στο καθολικό πραγματοποιείται μέσω αλγορίθμων συναίνεσης. Οι κόμβοι αυτοί ονομάζονται πλήρεις κόμβοι (full nodes). Οι αλγόριθμοι συναίνεσης μπορεί να διαφέρουν από blockchain σε blockchain ανάλογα με το είδος της πληροφορίας που καταγράφεται και το εάν το δίκτυο είναι δημόσιο ή ιδιωτικό. Στο bitcoin για παράδειγμα καταγράφονται συναλλαγές στο κρυπτονόμισμα bitcoin (BTC) οι οποίες πριν προσαρτηθούν στο blockchain θα πρέπει να επαληθευτούν μέσω ενός ισχυρού αλγορίθμου συναίνεσης που ονομάζεται POW (Proof Of Work). Οι πλήρεις κόμβοι διαθέτουν υπολογιστική ισχύ σε αντάλλαγμα του να τους δοθεί η δυνατότητα να επαληθεύουν συναλλαγές και συνεπώς να έχουν τη πιθανότητα να κερδίσουν ως ανταμοιβή κάποια bitcoins. Από την άλλη μεριά και σε ένα ιδιωτικό blockchain μπορούν να καταγράφονται συναλλαγές. Σε αυτή την περίπτωση καθώς οι συμμετέχοντες έχουν γνωστή και επαληθεύσιμη ταυτότητα, μπορούν να χρησιμοποιηθούν ελαφρύτεροι και ταχύτεροι αλγόριθμοι συναίνεσης έτσι ώστε ο ρυθμός διεκπεραίωσης των συναλλαγών να είναι υψηλότερος.

3 Κρυπτογραφία

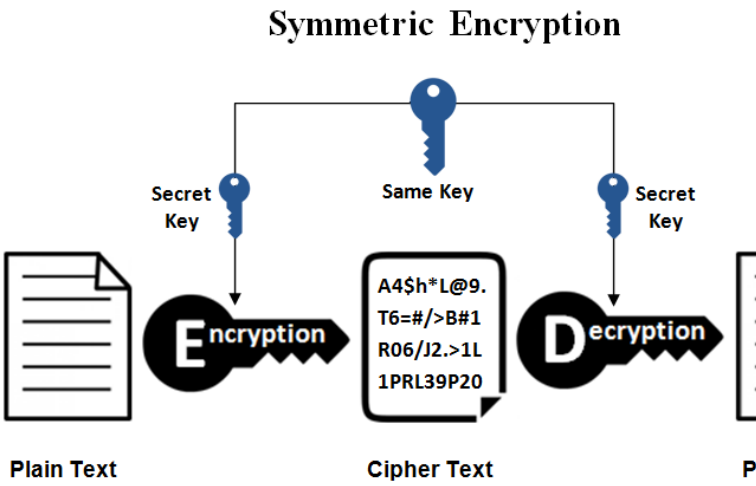
Η βασική ιδέα στην κρυπτογραφία είναι η προστασία των δεδομένων από άτομα που δεν έχουν την απαιτούμενη εξουσιοδότηση για αυτά. Κρυπτογράφηση είναι ο μετασχηματισμός των δεδομένων σε κρυπτογραφημένο κείμενο (cypher text) που αποτελεί ακατάληπτη μορφή για οποιονδήποτε δεν γνωρίζει πως να τα αποκρυπτογραφήσει. Αποκρυπτογράφηση είναι ο μετασχηματισμός του κρυπτογραφημένου κειμένου στο αρχικό κείμενο.

Η κρυπτογραφία χρησιμοποιείται έτσι ώστε να επιτευχθεί ταυτοποίηση (identification), πιστοποίηση (authentication) και εξουσιοδότηση (authorization). Η ταυτοποίηση έχει να κάνει με τον ισχυρισμό ότι κάποιος είναι ένα συγκεκριμένο άτομο. Η πιστοποίηση αφορά την απόδειξη ότι πράγματι κάποιος είναι αυτός που ισχυρίζεται. Η εξουσιοδότηση σχετίζεται με την πρόσβαση σε συγκεκριμένους πόρους λόγω της πιστοποίησης που έχει προηγηθεί.

3.1 Κατηγορίες μεθόδων κρυπτογραφίας

3.1.1 Συμμετρική κρυπτογραφία

Στη συμμετρική κρυπτογραφία χρησιμοποιείται ένα κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Χρησιμοποιείται και σήμερα αλλά παρουσιάζει προβλήματα που έχουν να κάνουν με τη διαχείριση των κλειδιών.

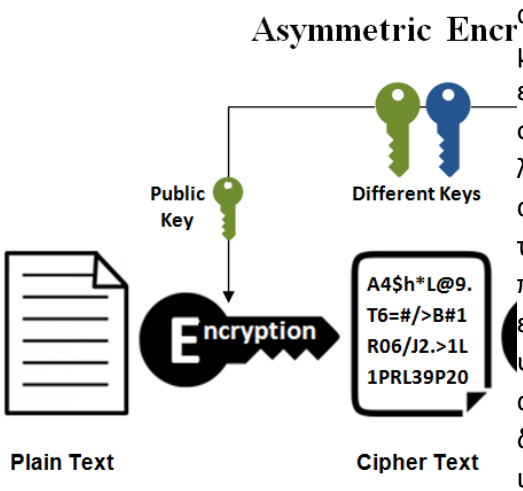


Εικόνα 2. Συμμετρική κρυπτογραφία

3.1.2 Ασύμμετρη κρυπτογραφία

Στην ασύμμετρη κρυπτογραφία χρησιμοποιούνται δύο συμπληρωματικά κλειδιά που το ένα ονομάζεται δημόσιο και το άλλο ιδιωτικό. Η επιλογή του ποιο κλειδί θα αποτελέσει το δημόσιο και ποιο το ιδιωτικό μπορεί να γίνει τυχαία και δεν επηρεάζει την κρυπτογράφηση. Δεδομένα τα οποία κρυπτογραφούνται με το δημόσιο κλειδί αποκρυπτογραφούνται με το ιδιωτικό κλειδί και δεδομένα που κρυπτογραφούνται με το ιδιωτικό κλειδί αποκρυπτογραφούνται με το δημόσιο κλειδί.

Από την στιγμή που έχουν δημιουργηθεί τα συμπληρωματικά κλειδιά το ένα ορίζεται ως δημόσιο και το άλλο ως ιδιωτικό. Το ιδιωτικό δεν δημοσιοποιείται στους άλλους αλλά το γνωρίζει μόνο ο κάτοχός του, ενώ το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο σε οποιονδήποτε ενδιαφερόμενο. Έτσι οποιοσδήποτε χρησιμοποιώντας το δημόσιο κλειδί μπορεί να κρυπτογραφήσει ένα μήνυμα που θα είναι σε θέση να το αποκρυπτογραφήσει μόνο ο κάτοχος του ιδιωτικού κλειδιού. Από την άλλη μεριά ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αποδείξει την ταυτότητά του καθώς μόνο αυτός μπορεί να στέλνει μηνύματα κρυπτογραφημένα με το ιδιωτικό του κλειδί τα οποία θα έχουν νόημα μόνο όταν αποκρυπτογραφηθούν από τους άλλους με το δημόσιο κλειδί που τους έχει δώσει.



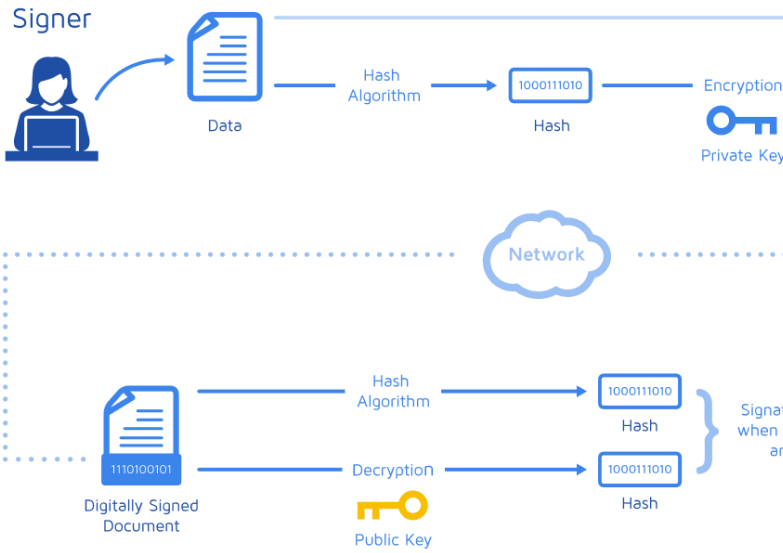
Εικόνα 3. Ασύμμετρη κρυπτογραφία

3.2 Η ασύμμετρη κρυπτογραφία στο blockchain

Η ασύμμετρη κρυπτογραφία χρησιμοποιείται για την αναγνώριση λογαριασμών και την εξουσιοδότηση συναλλαγών στο blockchain. Τα δεδομένα των συναλλαγών εμπεριέχουν δημόσια κλειδιά για την ταυτοποίηση των λογαριασμών (το δημόσιο κλειδί είναι και ο αριθμός του λογαριασμού). Από την άλλη μεριά ο ιδιοκτήτης του λογαριασμού που παραδίδει την ιδιοκτησία ενός πόρου μέσω μιας συναλλαγής κρυπτογραφεί ένα κείμενο με το ιδιωτικό του κλειδί. Οι άλλοι χρήστες μπορούν να επιβεβαιώσουν την ορθότητα της συναλλαγής χρησιμοποιώντας το δημόσιο κλειδί που όπως αναφέρθηκε παραπάνω είναι ο αριθμός του λογαριασμού του ιδιοκτήτη του πόρου που μεταβιβάζεται.

3.3 Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές επιτρέπουν τον έλεγχο σχετικά με το εάν ορισμένα δεδομένα ανήκουν σε κάποιον ο οποίος το ισχυρίζεται. Η δημιουργία μιας ψηφιακής υπογραφής γίνεται λαμβάνοντας την hash τιμή των δεδομένων και κρυπτογραφώντας την με το ιδιωτικό κλειδί του κατόχου των δεδομένων. Τόσο τα αρχικά δεδομένα όσο και η κρυπτογραφημένη τιμή (υπογραφή) τοποθετούνται μαζί σε ένα αρχείο και αποτελούν πλέον το ψηφιακά υπογεγραμμένο μήνυμα του κατόχου των δεδομένων. Η επαλήθευση ότι όντως τα δεδομένα ανήκουν σε αυτόν που το ισχυρίζεται γίνεται λαμβάνοντας το ψηφιακά υπογεγραμμένο αρχείο και εφαρμόζοντας μόνο στα δεδομένα του την hash συνάρτηση. Αν η τιμή που θα προκύψει είναι ίδια με την τιμή που θα επιστραφεί αποκρυπτογραφώντας την ψηφιακή υπογραφή που περιέχεται στο αρχείο τότε αυτό σημαίνει ότι πράγματι τα δεδομένα ανήκουν σε αυτόν που το είχε ισχυριστεί. Αντίστοιχα, η αναγνώριση απάτης είναι εύκολη καθώς οποιαδήποτε αλλαγή στα δεδομένα του αρχείου θα αλλάξει την hash τιμή των δεδομένων και πλέον δεν θα υπάρχει συμφωνία ανάμεσα σε αυτή και στην τιμή της αποκρυπτογραφημένης ψηφιακής υπογραφής. Τα παραπάνω φαίνονται σχηματικά στην Εικόνα 4.



Εικόνα 4. Ψηφιακή υπογραφή για επαλήθευση της ταυτότητας του υπογράφοντος[6]

3.4 Απόδειξη μηδενικής γνώσης (ZKP)

Η απόδειξη μηδενικής γνώσης (ZKP=Zero Knowledge Proof) είναι μια μέθοδος που επιτρέπει σε ένα άτομο (prover) να αποδείξει σε ένα άλλο άτομο (verifier) ότι ο πρώτος έχει

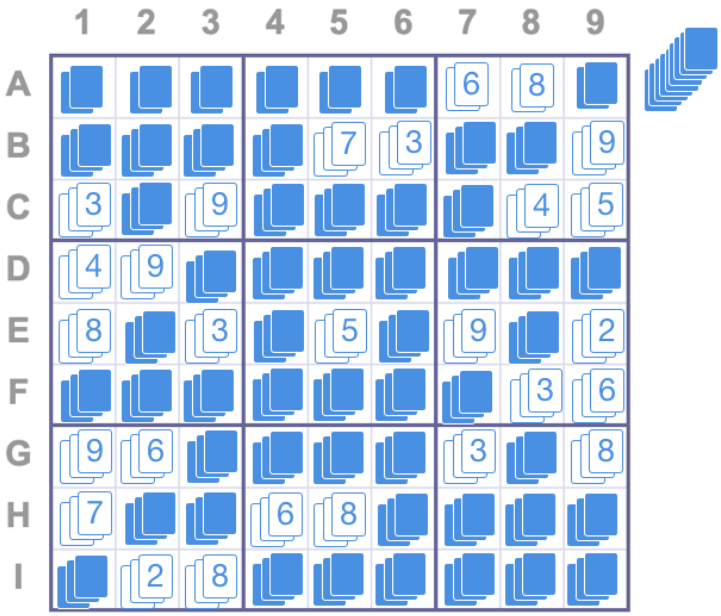
[6] https://medium.com/@meruja/digital-signature-generation-75cc63b7e1b4

στην κατοχή του κάποια πληροφορία χωρίς ο δεύτερος να μάθει στοιχεία της πληροφορίας. Η βασική ιδέα των ZKP διατυπώθηκε για πρώτη φορά στο [6]. Μια ZKP θα πρέπει να διαθέτει τις ακόλουθες ιδιότητες:

- Πληρότητα: Σε περίπτωση που ο verifier επαληθεύσει ότι ο prover κατέχει την πληροφορία τότε όντως ο prover κατέχει την πληροφορία.
- Ορθότητα: Αν ο prover δεν έχει στην κατοχή του την πληροφορία που προσπαθεί να πείσει τον verifier ότι έχει, ο verifier δεν μπορεί να πειστεί (παρά μόνο με μια απειροελάχιστη πιθανότητα).
- Μηδενική γνώση: Αν ο prover κατέχει την πληροφορία που ισχυρίζεται και ο verifier το επαληθεύει, κατά τη διαδικασία επαλήθευσης ο verifier δεν μαθαίνει τίποτα για την ίδια την πληροφορία πέρα από το γεγονός ότι βρίσκεται στην κατοχή του prover.

Ένα κλασσικό παράδειγμα επίδειξης του τρόπου λειτουργίας του ZKP είναι η απόδειξη ότι κάποιος διαθέτει μια λύση για ένα στιγμιότυπο προβλήματος του παιχνιδιού SUDOKU[7] χωρίς όμως να αποκαλύπτει την ίδια τη λύση που έχει εντοπίσει. Σε αυτή την περίπτωση ο verifier τυχαία επιλέγει να επαληθεύσει χρησιμοποιώντας κάποια στήλη κάποια σειρά ή κάποια ομάδα 9 κελιών από τις 9 που διαθέτει το παιχνίδι. Ο έλεγχος δεν αφορά τη συγκεκριμένη διαμόρφωση αλλά απλά ανιχνεύει ότι όλα τα ψηφία από το 1 μέχρι το 9 συμπεριλαμβάνονται. Για παράδειγμα, όπως φαίνεται και στην Εικόνα 5 η επαλήθευση μπορεί να αφορά τη σειρά 1 οπότε ο verifier συλλέγει τις κάρτες, τις ανακατεύει και στη συνέχεια ελέγχει ότι περιέχονται όλα τα ψηφία από το 1 μέχρι το 9, γυρίζοντας ανάποδα τα κρυφά φύλλα. Αν ο έλεγχος επαναληφθεί πολλές φορές για

Ένα σύστημα ZKP μπορεί να χρησιμοποιηθεί για παράδειγμα έτσι ώστε να μη χρειάζεται να δίνεται ο αριθμός της πιστωτικής κάρτας από τον ιδιοκτήτη της κάρτας σε έναν έμπορο και ωστόσο ο έμπορος να είναι σε θέση να διαπιστώσει ότι η κάρτα ανήκει ή δεν ανήκει σε εκείνον που το ισχυρίζεται.



Εικόνα 5. Zero Knowledge Proof (Sudoku)[8]

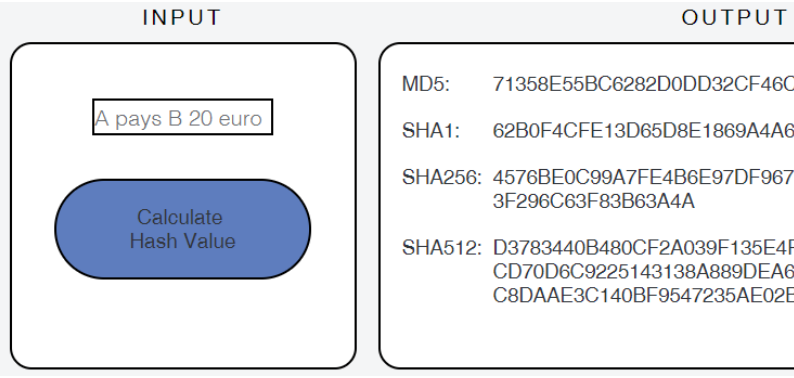
[7] https://en.wikipedia.org/wiki/Sudoku

[8] https://blog.goodaudience.com/understanding-zero-knowledge-proofs-through-simple-examples-df673f796d99

4 Κατακερματισμός

4.1 Συναρτήσεις κατακερματισμού

Οι συναρτήσεις κατακερματισμού (hash functions) είναι μικρά προγράμματα που μετασχηματίζουν οποιοδήποτε είδος και ποσότητα δεδομένων σε ακολουθίες ψηφίων σταθερού μήκους. Οι συναρτήσεις κατακερματισμού θα πρέπει να εκτελούνται ταχύτατα, να είναι ντετερμινιστικές δηλαδή για την ίδια είσοδο να παράγουν την ίδια έξοδο και για παραπλήσιες εισόδους να επιστρέφουν τιμές αρκετά διαφορετικές μεταξύ τους.



Εικόνα 6. Τιμές επιστροφής κρυπτογραφικών συναρτήσεων κατακερματισμού[9] για το κείμενο "A pays B 20 euro"

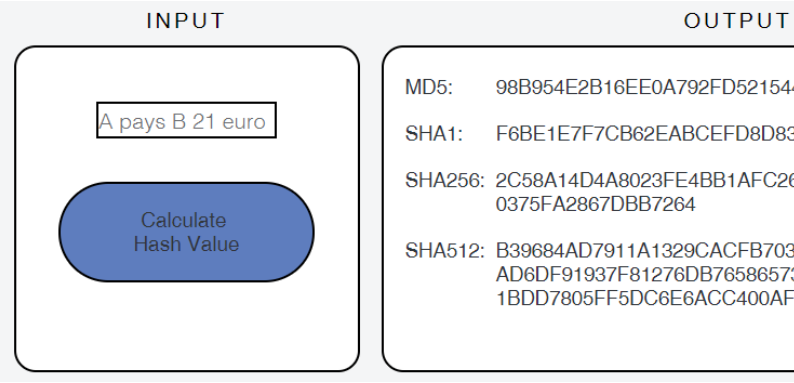
Υπάρχουν πολλές συναρτήσεις κατακερματισμού και μια σημαντική κατηγορία συναρτήσεων κατακερματισμού είναι οι κρυπτογραφικές συναρτήσεις. Μια καλή κρυπτογραφική συνάρτηση κατακερματισμού θα πρέπει να έχει επιπλέον τις ακόλουθες ιδιότητες:

- Να είναι μιας κατεύθυνσης (one-way).
- Να είναι ανθεκτική σε συγκρούσεις.
- Να είναι ψευδοτυχαία

Μια συνάρτηση είναι μιας κατεύθυνσης όταν δεν είναι δυνατόν να υπολογιστεί η είσοδος δεδομένης της εξόδου που έχει παραχθεί από τη συνάρτηση. Ανθεκτική σε συγκρούσεις σημαίνει ότι είναι δύσκολο και εξαιρετικά απίθανο να εντοπιστούν δύο οι περισσότερα στιγμιότυπα εισόδου που να επιστρέφουν το ίδιο αποτέλεσμα ως έξοδο. Τέλος, ψευδοτυχαία σημαίνει ότι η τιμή που επιστρέφεται από τη συνάρτηση κατακερματισμού αλλάζει με μη προβλέψιμο τρόπο κάθε φορά που η είσοδος αλλάζει.

Στην Εικόνα 6 φαίνεται η hash τιμή που επιστρέφουν τέσσερις διαφορετικές κρυπτογραφικές συναρτήσεις κατακερματισμού (MD5, SHA1, SHA256, SHA512) για το κείμενο "A pays B 20 euro".

Οποιαδήποτε αλλαγή στο κείμενο της εισόδου αλλάζει πλήρως τις επιστρεφόμενες τιμές. Για παράδειγμα στην Εικόνα 7 φαίνονται οι νέες τιμές που προκύπτουν όταν το κείμενο αλλάξει από "A pays B 20 euro" σε "A pays B 21 euro".



Εικόνα 7. Τιμές επιστροφής κρυπτογραφικών συναρτήσεων κατακερματισμού για το κείμενο "A pays B 21 euro"

Υπάρχουν διάφοροι μηχανισμοί έτσι ώστε οι συναρτήσεις κατακερματισμού να μπορούν να εφαρμοστούν και σε δεδομένα που αποτελούν σύνθεση άλλων ανεξάρτητων τμημάτων δεδομένων όπως για παράδειγμα τα δεδομένα πολλών συναλλαγών και να επιστρέψουν μια hash τιμή για το σύνολο των δεδομένων. Ένας αποδοτικός μηχανισμός για να επιτευχθεί αυτό είναι τα Merkle Trees τα οποία θα αναφερθούν στη συνέχεια.

[9] http://www.blockchain-basics.com/HashFunctions.html

4.2 Εφαρμογές κατακερματισμού

Ο κατακερματισμός έχει πολλές πρακτικές εφαρμογές. Ορισμένες από αυτές είναι οι ακόλουθες:

- Σύγκριση δεδομένων
- Ανίχνευση αλλαγών σε δεδομένα
- Αποθήκευση δεδομένων με δυνατότητα ανίχνευσης αλλαγών
- Εκτέλεση υπολογιστικά δύσκολων εργασιών

4.2.1 Σύγκριση δεδομένων

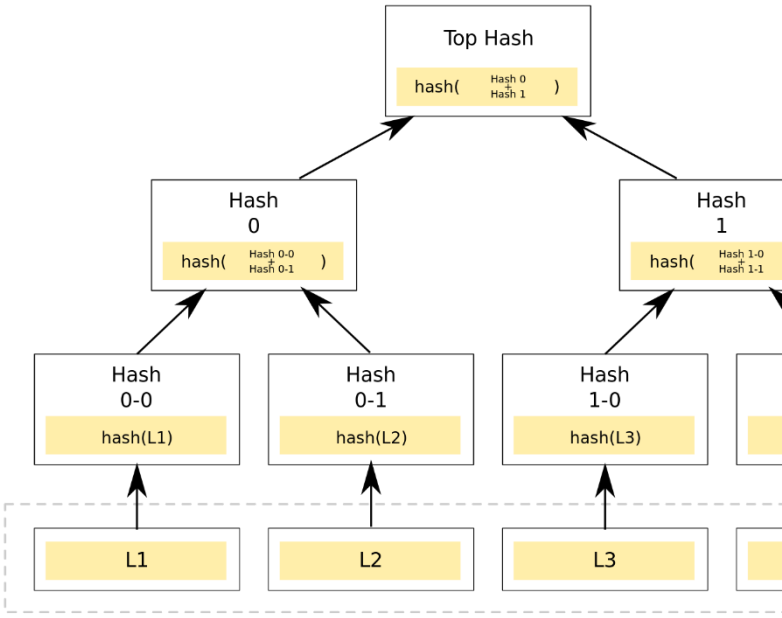
Οι συναρτήσεις κατακερματισμού μπορούν να χρησιμοποιηθούν για τη σύγκριση δεδομένων. Αν για παράδειγμα υπάρχει ένα σύνολο κειμένων και ζητείται να εντοπιστούν τα κείμενα που είναι ίδια, τότε μπορεί να υπολογιστεί η κρυπτογραφική hash τιμή του κάθε κειμένου και στη συνέχεια να αναχθεί η σύγκριση των κειμένων στην σύγκριση των hash τιμών. Το αποτέλεσμα αναμένεται να είναι σωστό λόγω της ανθεκτικότητας σε συγκρούσεις που παρουσιάζουν οι κρυπτογραφικές hash συναρτήσεις.

4.2.2 Ανίχνευση αλλαγών σε δεδομένα

Υπολογίζοντας την κρυπτογραφική hash τιμή ορισμένων δεδομένων σε κάποια χρονική στιγμή και υπολογίζοντας την ξανά σε κάποια άλλη χρονική στιγμή μπορεί να ληφθεί συμπέρασμα για το εάν τα δεδομένα παραμείνουν τα ίδια ή αν έχουν υποστεί αλλαγές η οποία έχει συντελεστεί ανάμεσα στις δύο αυτές χρονικές στιγμές. Αν οι hash τιμές είναι ίδιες τότε τα δεδομένα δεν έχουν τροποποιηθεί ενώ αν διαφέρουν τα δεδομένα έχουν τροποποιηθεί.

4.2.3 Αποθήκευση δεδομένων με δυνατότητα ανίχνευσης αλλαγών

Επιμέρους μπλοκ δεδομένων που αποτελούν όλα μαζί ένα μεγαλύτερο μπλοκ δεδομένων μπορούν να συνδυαστούν σε μια δενδρική δομή που ονομάζεται Merkle Tree έτσι ώστε σε περίπτωση που οποιοδήποτε από τα επιμέρους μπλοκ δεδομένων αλλάξει να είναι δυνατή η ανίχνευση του γεγονότος της αλλαγής στο σύνολο των δεδομένων. Για παράδειγμα στην Εικόνα 8 για καθένα από τα 4 μπλοκ δεδομένων L1, L2, L3 και L4 δημιουργείται από μια hash τιμή. Οι hash τιμές συνδυάζονται ανά δύο και εφαρμόζεται σε αυτό το συνδυασμό εκ νέου η hash συνάρτηση. Αυτό συνεχίζεται σε επίπεδα και μέχρι να προκύψει στην ρίζα (δηλαδή στο υψηλότερο κόμβο) του δένδρου μια hash τιμή που αντιπροσωπεύει το σύνολο των δεδομένων. Το ιδιαίτερο χαρακτηριστικό του Merkle Tree είναι ότι αν οποιοδήποτε από τα επιμέρους μπλοκ δεδομένων που βρίσκονται στη βάση του δένδρου τροποποιηθεί τότε αυτόματα αλλάζει και η hash τιμή στη ρίζα του δένδρου.



Εικόνα 8. Merkle δένδρο[10]

Η αποθήκευση δεδομένων συναλλαγών με τρόπο που να είναι ανιχνεύσιμη η αλλαγή σε μια οποιαδήποτε από τις επιμέρους συναλλαγές που συνιστούν ένα μπλοκ βρίσκει εφαρμογή στο blockchain.

4.2.3.1 Εκτέλεση υπολογιστικά δύσκολων εργασιών

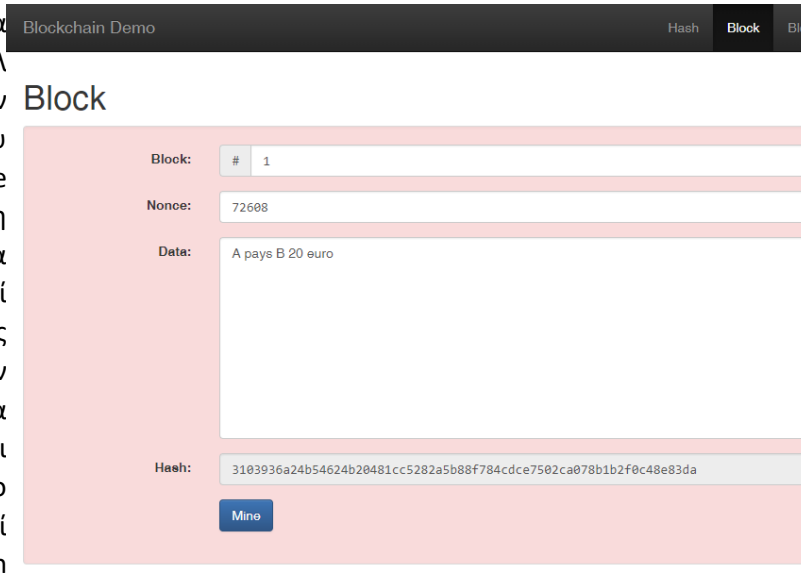
Μια εφαρμογή των συναρτήσεων κατακερματισμού σε διαφορετική

[10] https://en.wikipedia.org/wiki/Merkle_tree

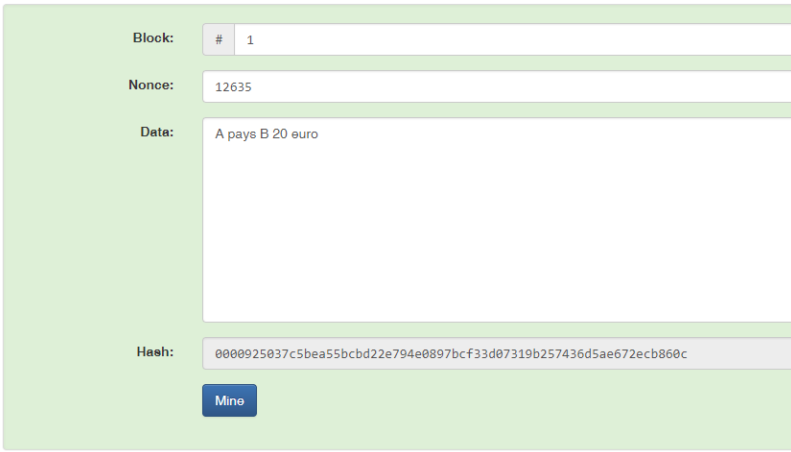
κατεύθυνση από τις προηγούμενες είναι τα λεγόμενα hash puzzles. Σε ένα hash παζλ δίνονται κάποια δεδομένα που δεν μπορούν να τροποποιηθούν, κάποια δεδομένα που επιτρέπεται να αλλάξουν και λέγονται nonce και μια κρυπτογραφική συνάρτηση κατακερματισμού. Ζητείται να παραχθεί μια hash τιμή για τα δεδομένα και το nonce μαζί που να πληροί συγκεκριμένα κριτήρια όπως για παράδειγμα να ξεκινά με έναν συγκεκριμένο αριθμό μηδενικών. Τα κριτήρια βάσει των οποίων μια λύση θεωρείται αποδεκτή καθορίζουν και το επίπεδο δυσκολίας του παζλ. Θα πρέπει να σημειωθεί ότι τα hash παζλ στα πλαίσια του blockchain ονομάζονται Proof of Work.

Το ιδιαίτερο χαρακτηριστικό των hash puzzles είναι ότι ο μόνος τρόπος με τον οποίο μπορούν να επιλυθούν είναι δοκιμάζοντας διαφορετικές τιμές για το nonce μέχρι για κάποια τιμή του nonce να επιτευχθεί hash τιμή που να ικανοποιεί τους περιορισμούς. Εφόσον βρεθεί το κατάλληλο nonce η επαλήθευση ότι όντως είναι έγκυρο από οποιονδήποτε άλλον είναι εξαιρετικά εύκολη. Αρκεί να συνδυάσει τα δεδομένα εισόδου με το nonce, να εφαρμόσει την hash συνάρτηση και να διαπιστώσει ότι όντως ικανοποιεί τους περιορισμούς που έχουν τεθεί.

Στην Εικόνα 9 παρουσιάζεται ένα μπλοκ πριν λυθεί το hash παζλ ενώ στην Εικόνα 10 παρουσιάζεται το ίδιο μπλοκ στο οποίο έχει πραγματοποιηθεί εξόρυξη (mining) και έχει πλέον εντοπιστεί μια τιμή nonce για την οποία η hash τιμή του μπλοκ ξεκινά με 4 μηδενικά.



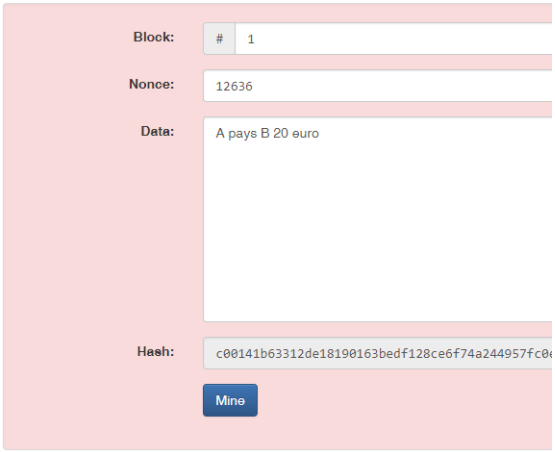
Εικόνα 9. Ένα μπλοκ πριν λυθεί το hash puzzle (μη έγκυρο nonce)[11]



Εικόνα 10. Ένα μπλοκ με έγκυρο nonce που επιλύει ένα hash puzzle δυσκολίας 4

Οποιαδήποτε αλλαγή στο nonce ή στα δεδομένα καθιστά την τρέχουσα τιμή hash μη έγκυρη. Αυτό φαίνεται στην Εικόνα 11 όπου έχει πραγματοποιηθεί χειροκίνητη αλλαγή στο nonce σε μια τιμή διαφορετική από την τιμή 12635 που είχε εξορυχθεί. Λόγω αυτής της αλλαγής η hash τιμή του μπλοκ πλέον δεν ξεκινά με τα απαιτούμενα 4 μηδενικά. Το ίδιο θα συνέβαινε και σε πιθανή αλλαγή τον δεδομένων του μπλοκ.

[11] https://anders.com/blockchain/blockchain.html



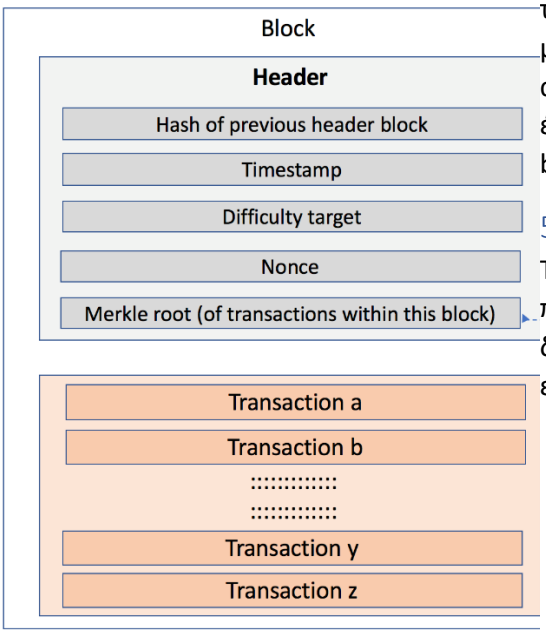
Εικόνα 11. Απόπειρα αλλαγής του nonce από 12635 σε 12636

5 Blockchain

Το blockchain είναι ένα αποκεντρωμένο καθολικό που μπορεί να χρησιμοποιηθεί για την αποθήκευση οποιουδήποτε είδους πληροφορίας. Ένα blockchain αποτελείται από μια αλυσίδα μπλοκς και μια κεφαλή (blockchain head).

5.1 Η δομή των μπλοκς

Κάθε μπλοκ διαθέτει μια κεφαλίδα (block header) Εικόνα 12 και ένα Merkle tree που περιέχει δεδομένα συναλλαγών.



Εικόνα 12. Η δομή ενός μπλοκ[12]

Τα περιεχόμενα της επικεφαλίδας κάθε μπλοκ είναι:

- Μια hash αναφορά στην επικεφαλίδα του προηγούμενου μπλοκ.
- Η χρονική στιγμή στην οποία ξεκίνησε η επίλυση του hash puzzle
- Το επίπεδο δυσκολίας του hash puzzle
- Το nonce που λύνει το hash puzzle
- Η ρίζα του Merkle tree που περιέχει τα δεδομένα των συναλλαγών

Συνεπώς, η σύνδεση μεταξύ των μπλοκς σε μια αλυσίδα γίνεται μέσω των hash αναφορών στις επικεφαλίδες των μπλοκς, με κάθε μπλοκ να διατηρεί σύνδεση με την hash αναφορά του προηγούμενού του μπλοκ. Η δε κεφαλή του blockchain έχει ως τιμή την hash αναφορά στην επικεφαλίδα του πλέον πρόσφατα εισηγμένου μπλοκ.

Η πρώτη συναλλαγή σε ένα μπλοκ είναι μια ειδική συναλλαγή που ονομάζεται «συναλλαγή coinbase» στην οποία τοποθετείται η εν δυνάμει αμοιβή την οποία θα λάβει ο miner εφόσον επιλύσει το μπλοκ. Στην περίπτωση του Bitcoin η αμοιβή αυτή με τις τρέχουσες τιμές είναι 12.5 bitcoins και μπορεί να χρησιμοποιηθεί μόνο εάν το μπλοκ αποτελέσει μέρος του blockchain και αφού έχουν προστεθεί 100 ακόμα μπλοκς στο blockchain.

5.2 Δημιουργία ενός νέου μπλοκ

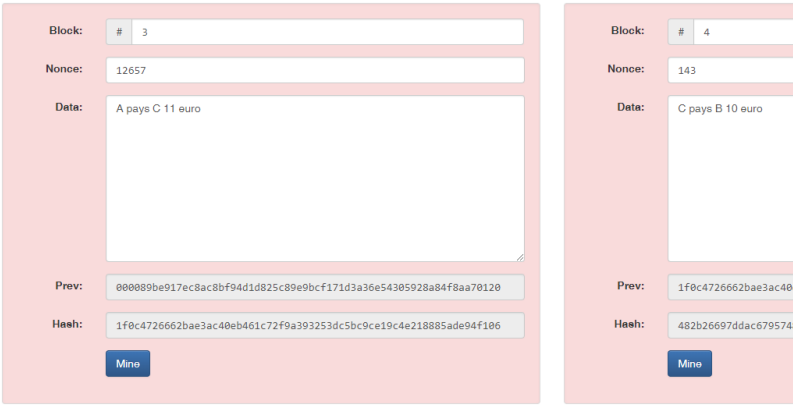
Τα βήματα που απαιτούνται προκειμένου να προστεθεί ένα νέο μπλοκ που περιέχει δεδομένα νέων συναλλαγών στο blockchain είναι τα ακόλουθα:

1. Δημιουργία ενός Merkle Tree που περιέχει τα δεδομένα των νέων συναλλαγών που πρόκειται να προστεθούν
2. Δημιουργία μιας κεφαλίδας μπλοκ που περιέχει το hash του προηγούμενου μπλοκ και τη ρίζα του Merkle Tree
3. Δημιουργία μιας hash τιμής για την κεφαλίδα του νέου μπλοκ η οποία αποτελεί πλέον την τρέχουσα κεφαλή του blockchain

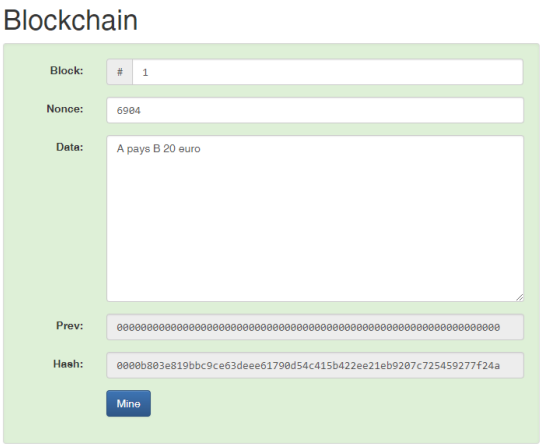
Στην Εικόνα 13 και στην Εικόνα 14 παρουσιάζεται ένα blockchain με 4 μπλοκς. Για την εισαγωγή κάθε μπλοκ εντοπίστηκε η τιμή nonce που έλυνε το αντίστοιχο hash puzzle. Στην Εικόνα 15 ένας υποτιθέμενος κακόβουλος χρήστης έχει αλλάξει τα δεδομένα του μπλοκ 3. Αυτό καθιστά αμέσως τόσο το μπλοκ 3 ως μη έγκυρο αλλά επίσης και το μπλοκ 4. Για να ολοκληρωθεί η προσπάθεια

[12] https://luxsci.com/blog/understanding-blockchains-and-bitcoin-technology.html

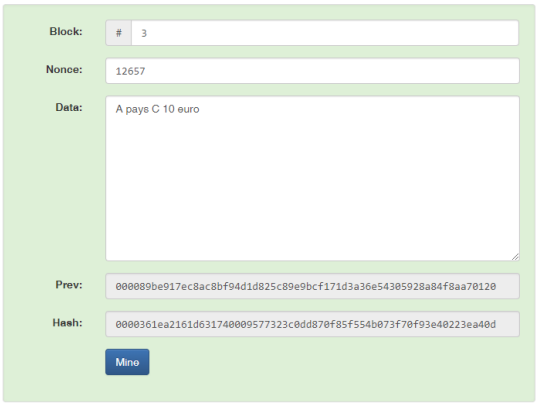
παραχάραξης θα έπρεπε να εξορυχθεί ένα νέο nonce πρώτα για το μπλοκ 3 και εν συνεχεία για το μπλοκ 4. Ακόμα και σε αυτή την περίπτωση ο κακόβουλος χρήστης θα έπρεπε να «πείσει» το δίκτυο ότι η δική του έκδοση του blockchain είναι η έγκυρη. Η μεγάλη υπολογιστική προσπάθεια που πρέπει να διατεθεί για να πραγματοποιηθεί μια αλλαγή στο blockchain καθιστά στην πράξη το blockchain μη μεταλλάξιμο (immutable) με δυνατότητα προσθήκης μόνο νέων δεδομένων.



Εικόνα 15. Προσπάθεια αλλαγής των δεδομένων στο μπλοκ 3 που καθιστά μη έγκυρα τα μπλοκ 3 και 4



Εικόνα 13. Τα δύο πρώτα μπλοκ (1 και 2) ενός blockchain με 4 μπλοκ



Εικόνα 14. Τα 2 επόμενα μπλοκ (3 και 4) του blockchain

Συνήθως το επίπεδο δυσκολίας των hash puzzles που καλούνται να επιλύσουν οι miners ορίζεται δυναμικά ανάλογα με την ταχύτητα με την οποία προστίθενται νέα μπλοκς.

5.3 Κατανομή του blockchain στο δίκτυο

Η αξία του blockchain ως δομής αποθήκευσης συναλλαγών είναι περιορισμένη αν θεωρηθεί ότι διατηρείται σε έναν μόνο υπολογιστή. Στην πραγματικότητα διατηρούνται πολλά συγχρονισμένα μεταξύ τους αντίγραφα του blockchain σε επιμέρους κόμβους (υπολογιστές χρηστών) που συνδέονται μεταξύ τους μέσω ενός δικτύου. Το δε δίκτυο που συνήθως χρησιμοποιείται είναι το Internet καθώς αποτελεί μια φθηνή λύσης δικτύωσης. Η επικοινωνία μεταξύ των κόμβων γίνεται μέσω μηνυμάτων που οι κόμβοι στέλνουν στους άλλους κόμβους ενημερώνοντάς τους για αλλαγές στο blockchain. Κάθε κόμβος διατηρεί μια λίστα άλλων ομότιμων κόμβων με τους οποίους επικοινωνεί απευθείας. Η λίστα αυτή αποτελεί υποσύνολο των κόμβων του δικτύου. Εάν κάποιος από τη λίστα κόμβων δεν αποκρίνεται σε μηνύματα τότε αντικαθίσταται από κάποιον άλλο κόμβο. Έτσι, όταν ένας νέος κόμβος προστίθεται στο σύστημα, αυτόματα δημιουργείται για αυτόν ένας αριθμός συνδέσεων με άλλους κόμβους που είναι ήδη μέλη τους συστήματος.

Το σύστημα χρησιμοποιεί ένα σύστημα αμοιβών οι οποίες λαμβάνονται σε ένα ανταγωνιστικό για τους κόμβους περιβάλλον έτσι ώστε να διασφαλιστεί ότι το blockchain περιέχει μόνο έγκυρα δεδομένα. Ο ρόλος των κόμβων είναι διπλός. Αφενός, ένας κόμβος ελέγχει την εγκυρότητα των μπλοκ που έχουν δημιουργηθεί από κάποιον άλλο ομότιμο κόμβο και αφετέρου προσπαθεί να δημιουργήσει το δικό του μπλοκ που θα πρέπει να ελεγχθεί από τους άλλους κόμβους. Ειδικότερα, τα βήματα που ακολουθούνται για την καταγραφή δεδομένων στο blockchain είναι τα ακόλουθα:

1. Κάθε κόμβος λαμβάνει δεδομένα νέων συναλλαγών καθώς και νέα μπλοκς προς επαλήθευση και αναλαμβάνει να τα προωθήσει στους κόμβους με τους οποίους επικοινωνεί απευθείας.
2. Αν ένας κόμβος λάβει ένα νέο μπλοκ για επαλήθευση το επεξεργάζεται κατά προτεραιότητα.
3. Τα δεδομένα συναλλαγών που λαμβάνει ο κάθε κόμβος συγκεντρώνονται σε ένα Merkle tree δημιουργώντας ένα νέο μπλοκ για το οποίο θα πρέπει να λυθεί το σχετικό με αυτό hash puzzle. Όταν ο κόμβος επιλύσει το hash puzzle το στέλνει προς επιβεβαίωση στους άλλους κόμβους.
4. Κάθε κόμβος προσθέτει νέα έγκυρα μπλοκς στο δικό του αντίγραφο του blockchain.
5. Αν προστεθεί ένα νέο μπλοκ στο blockchain όλες οι συναλλαγές που περιέχει αφαιρούνται από τις συναλλαγές με τις οποίες ο κόμβος προσπαθούσε να κατασκευάσει το δικό του νέο μπλοκ.
6. Ο κόμβος του οποίου το μπλοκ εισάγεται στο blockchain κερδίζει την αμοιβή που έχουν όλες οι συναλλαγές που εμπεριέχονται στο μπλοκ.

5.4 Κυρίαρχο ιστορικό συναλλαγών

Καθώς κάθε κόμβος του δικτύου διατηρεί το πλήρες ιστορικό των συναλλαγών θα πρέπει να αντιμετωπιστεί το θέμα της συμφωνίας σε ένα κοινά αποδεκτό ιστορικό συναλλαγών από όλα τα μέλη του δικτύου. Ο τρόπος με τον οποίο οι κόμβοι θα καταλήγουν σε συμφωνία δεν θα πρέπει να εμπλέκει κάποια κεντρική οντότητα.

Η βασική ιδέα είναι ότι το κριτήριο επιλογής ανάμεσα σε εναλλακτικά ιστορικά συναλλαγών είναι ο φόρτος που έχει δαπανηθεί για τη δημιουργία τους, επιλέγοντας εκείνο για το οποίο έχει δαπανηθεί ο μεγαλύτερος υπολογιστικά φόρτος. Συχνά αυτό αναφέρεται ως «κριτήριο της μακρύτερης αλυσίδας» καθώς το blockchain με τα περισσότερα μπλοκς συνεπάγεται και υψηλότερο φόρτο για τη δημιουργία του. Αν δύο ή περισσότερα ιστορικά συναλλαγών έχουν το ίδιο μεγαλύτερο μήκος τότε θεωρούνται εν δυνάμει έγκυρα ενώ οποιοδήποτε ιστορικό συναλλαγών πάψει να έχει μήκος τουλάχιστον ίσο με το μήκος της μακρύτερης εναλλακτικής αλυσίδας απορρίπτεται.

Καθώς το επίπεδο δυσκολίας για την επίλυση των hash παζλ είναι μεταβλητό συνήθως το «κριτήριο της μακρύτερης αλυσίδας» μετασχηματίζεται στο «κριτήριο της βαρύτερης αλυσίδας». Σύμφωνα με αυτό επιλέγεται το ιστορικό συναλλαγών που αναπαριστά μια αλυσίδα μπλοκς για την οποία χρειάστηκε μεγαλύτερος φόρτος για να δημιουργηθεί χωρίς κατ' ανάγκη να είναι και η μακρύτερη αλυσίδα.

Καθώς προστίθενται συναλλαγές στο blockchain, δημιουργούνται αλυσίδες συναλλαγών που διακλαδίζονται μέχρι το σημείο που κάποια από τις διακλαδώσεις αποκτά μεγαλύτερο μήκος (ή βάρος). Τα μπλοκς που ανήκουν σε διακλαδώσεις που εγκαταλείπονται ονομάζονται ορφανά και αφαιρούνται λογικά από το blockchain ενώ διατηρούνται στην ίδια τη δομή δεδομένων η οποία μοιάζει περισσότερο με δένδρο παρά

με αλυσίδα. Οι συναλλαγές που καταλήγουν σε ορφανά μπλοκ εισάγονται ξανά στο blockchain. Οι συναλλαγές που ανήκουν στην κυρίαρχη (authoritative) αλυσίδα θεωρείται ότι έχουν πραγματοποιηθεί αν και το blockchain μπορεί να μην είναι μόνο να εγγυηθεί τη λεγόμενη συνέπεια μέλλον (eventual consistency) που σημαίνει ότι η συμμετοχή των συναλλαγών στα μπλοκ καθώς περνά ο χρόνος από τη στιγμή που εισήχθησαν στο σύστημα.

Ο παραπάνω τρόπος λειτουργίας μπορεί να δεχθεί τη λεγόμενη «επίθεση του 51 τοις εκατό». Σύμφωνα με αυτή αν συνεργαστεί το 51% των χρηστών του δικτύου τότε μπορούν να επιλεγούν συγκεκριμένες συναλλαγές που ωφελούν κάποιο ή κάποια μέλη και να αποτελέσουν το περιεχόμενο μπλοκς της κυρίαρχης αλυσίδας.

Θεωρείται γενικά ότι μια συναλλαγή που είναι σε ένα μπλοκ που βρίσκεται 6 μπλοκς ή περισσότερο βαθιά στο blockchain έχει επιβεβαιωθεί. Οποιαδήποτε εναλλακτικό blockchain θα ήταν υπολογιστικά ασύμφορο να δημιουργηθεί έτσι ώστε να τροποποιήσει ή να ακυρώσει τη συγκεκριμένη συναλλαγή.

5.5 Μειονεκτήματα του blockchain

Σύμφωνα με τα παραπάνω, το blockchain είναι ένα πλήρως ομότιμο σύστημα που επιτρέπει σε οποιονδήποτε να διαβάσει το ιστορικό των συναλλαγών και να προσθέσει τις δικές του συναλλαγές οι οποίες ενσωματώνονται σε μια δομή δεδομένων που διατηρείται συλλογικά από τα μέλη του δικτύου. Συνεπώς, όλα τα στοιχεία των συναλλαγών είναι διαθέσιμα σε όλους και το γεγονός αυτό καθιστά προβληματική τη χρήση του blockchain σε περιπτώσεις που απαιτούνται υψηλά επίπεδα ιδιωτικότητας (privacy). Βέβαια, οι αριθμοί λογαριασμών είναι δημόσια κρυπτογραφικά κλειδιά και όχι πραγματικά ονόματα ή διευθύνσεις. Ωστόσο, αν για οποιοδήποτε λόγο το ιδιωτικό κλειδί ενός λογαριασμού δοθεί σε άλλους τότε η ασφάλεια του λογαριασμού καταρρέει.

Ένα άλλο σημείο προβληματισμού έχει να προσκάνει με τις δυνατότητες κλιμάκωσης του δεσυστήματος. Ο μηχανισμός επαλήθευσης των συναλλαγών μέσω της επίλυσης hash παζλ αλυσίδα θεωρείται ότι έχουν περαίωσης συναλλαγών που μπορεί να μην είναι μόνο να εγγυηθεί τη λεγόμενη συνέπεια στο δεκτά για ορισμένα είδη εφαρμογών. Επιπλέον, το κόστος αγοράς εξειδικευμένου εξοπλισμού και το κόστος κατανάλωσης ηλεκτρικού ρεύματος είναι ιδιαίτερα υψηλά.

Από την άλλη μεριά, υπάρχουν θέματα νομικής φύσεως που σχετίζονται με το ποιος έχει την ευθύνη απέναντι στο νόμο για την επιβεβαίωση των συναλλαγών δεδομένου του συλλογικού τρόπου με τον οποίο επαλήθευση. Το γεγονός αυτό προκαλεί ανασφάλεια στους πιθανούς χρήστες και περιορίζει τον αριθμό των χρηστών που επιλέγουν να χρησιμοποιήσουν την τεχνολογία blockchain.

Αναλυτικότερη αναφορά στον προβληματισμό που υπάρχει για την τεχνολογία blockchain και ποιες συνθήκες την εφαρμογές υπάρχει στο κεφάλαιο 9.

6 Κρυπτονομίσματα

Η χρήση μετρητών θεωρείται σε μεγάλο βαθμό παρωχημένη και ένα μεγάλο μέρος των οικονομικών συναλλαγών γίνεται ψηφιακά με τις τράπεζες να αναλαμβάνουν τη διατήρηση, σε κλειστά για τους άλλους συστήματα, όλων εκείνων των δεδομένων που περιγράφουν τις συναλλαγές. Η τάση ψηφιοποίησης των συναλλαγών και περιορισμού της χρήσης των φυσικών νομισμάτων και χαρτονομισμάτων αναμένεται να συνεχιστεί εντονότερη στο άμεσο μέλλον λόγω του μετασχηματισμού των τραπεζών σε επιχειρήσεις τεχνολογίας. Τα κρυπτονομίσματα είναι πλήρως ψηφιακά νομίσματα που στηρίζονται στην κρυπτογραφία. Αν και στο παρελθόν έγιναν απόπειρες κυκλοφορίας ψηφιακών νομισμάτων που διέθεταν κάποια χαρακτηριστικά κρυπτονομισμάτων η πρώτη επιτυχημένη κυκλοφορία κρυπτονομίσματος θεωρείται ότι πραγματοποιήθηκε με το bitcoin. Αυτό επιτεύχθηκε επιβάλλοντας σε μέλη ενός ομότιμου (peer-to-peer) δικτύου να διαθέτουν σημαντική υπολογιστική ισχύ για επαλήθευση συναλλαγών και εν συνεχεία τη στοχαστική πληρωμή τους για την υπηρεσία αυτή.

6.1 Bitcoin

Τον Οκτώβριο του 2008 ένας ανώνυμος χάκερ με το ψευδώνυμο Satoshi Nakamoto δημοσιοποίησε τις ιδέες του για τη λειτουργία του πλήρως ψηφιακού κρυπτονομίσματος bitcoin [7]. Η δημοσιοποίηση των ιδεών του, που κατά βάση ήταν γνωστές ιδέες στην επιστημονική κοινότητα αλλά προσφέρθηκαν με ένα συνεκτικό τρόπο στοχεύοντας στην επίλυση ενός υπαρκτού προβλήματος, έγινε μέσω ενός white paper[13] το οποίο στάλθηκε σε μια λίστα αλληλογραφίας. Η έκδοση 0.1 του λογισμικού bitcoin διατέθηκε από τον Nakamoto στο αποθετήριο λογισμικού sourceforge στις 9 Ιανουαρίου του 2009. Ο Nakamoto δημιούργησε το website bitcoin.org και σε συνεργασία με άλλους προγραμματιστές συνέχισε την ανάπτυξη του λογισμικού bitcoin μέχρι τα μέσα του 2010 οπότε και αποσύρθηκε.

Ο σχεδιασμός του bitcoin επιτρέπει την αποτελεσματική αντιμετώπιση του προβλήματος της διπλής χρέωσης χρησιμοποιώντας ένα ομότιμο, κατανεμημένο σύστημα ικανό να επιβεβαιώνει μέσω υπολογισμών τη χρονολογική σειρά με την οποία δημιουργούνται οι συναλλαγές. Η φράση «διπλή χρέωση» (double spending) αναφέρεται στην ευκολία με την οποία μπορεί να αντιγραφεί η ψηφιακή πληροφορία και στο πρόβλημα που αυτό συνεπάγεται για τα ψηφιακά νομίσματα. Τα φυσικά νομίσματα (π.χ. νομίσματα και χαρτονομίσματα ευρώ) αντιμετωπίζουν σε πολύ μικρότερο βαθμό το πρόβλημα αυτό διότι είναι δύσκολο να αντιγραφούν και ακόμα και σε περίπτωση παραχάραξης τους τα συναλλασσόμενα μέλη είναι σε θέση να εντοπίσουν την απάτη με προσεκτική εξέταση των νομισμάτων. Επιπλέον η νομοθεσία επιβάλει σοβαρότατες ποινές για όποιους εμπλέκονται στο αδίκημα της παραχάραξης νομισμάτων. Ωστόσο, ένα ψηφιακό αντίγραφο είναι πλήρως πανομοιότυπο με την αρχική πηγή από την οποία προέκυψε. Το bitcoin εισήγαγε έναν μηχανισμό ο οποίος αποτρέπει τη διπλή χρέωση παρά το γεγονός ότι δεν υπάρχει κάποια κεντρική «έμπιστη» οντότητα που εγγυάται την ορθότητα των συναλλαγών. Αυτό επιτυγχάνεται μέσω του blockchain το οποίο στην περίπτωση του bitcoin αποτελείται από επιβεβαιωμένες συναλλαγές που τοποθετούνται σε blocks με το ένα block να συνδέεται με το επόμενο σε μια αλυσίδα. Η επιβεβαίωση των συναλλαγών είναι μια υπολογιστικά απαιτητική διαδικασία και η ασφάλεια του όλου συστήματος στηρίζεται στο ότι η προσπάθεια εισαγωγής εσφαλμένων δεδομένων στο blockchain κοστίζει υπερβολικά πολύ.

[13] white paper: έγγραφο που στοχεύει στην κατανόηση ενός σύνθετου θέματος, στην επίλυση ενός προβλήματος ή στη λήψη αποφάσεων για ένα συγκεκριμένο θέμα

Η λειτουργία του bitcoin για περισσότερο από 10 έτη έχει δείξει ότι ο συγκεκριμένος μηχανισμός είναι ιδιαίτερα αποτελεσματικός στο να αποτρέπει επίδοξους hackers από το να επιχειρούν αλλοίωση των δεδομένων των συναλλαγών. Ωστόσο, θα πρέπει να σημειωθεί ότι ο κίνδυνος της επίθεσης του 51% είναι υπαρκτός. Αυτό σημαίνει ότι σε περισσότερο από το 50% της υπολογιστικής ισχύος που συντηρεί το blockchain τότε είναι σε θέση να μεταφέρει bitcoins σε δικούς του λογαριασμούς καθώς ο ίδιος έχει την απαιτούμενη πλειοψηφία έτσι ώστε να επικυρώσει την «ορθότητα» των συναλλαγών που πραγματοποιούνται και το υπόλοιπο δίκτυο θα πρέπει να το αποδεχθεί. Ωστόσο, στην περίπτωση του bitcoin που σήμερα διαθέτει περί τους 30.000 κόμβους επαλήθευσης συναλλαγών αυτό σημαίνει ότι θα απαιτούταν η διάθεση υπερβολικής υπολογιστικής ισχύος.

6.1.1 Παράδειγμα συναλλαγής με bitcoins

Το blockchain του bitcoin είναι διαθέσιμο σε οποιονδήποτε διαθέτει σύνδεση στο διαδίκτυο ενώ ταυτόχρονα υπάρχουν πολλά αντίγραφά του bitcoin blockchain σε διάφορους υπολογιστές διάσπαρτους σε όλον τον κόσμο. Μια ειδική κατηγορία συμμετεχόντων στο δίκτυο είναι οι miners (εξορύκτες) που είναι υπεύθυνοι για τον εντοπισμό, τη συγκέντρωση και την επαλήθευση των συναλλαγών. Οι miners σχηματίζουν με τα στοιχεία των συναλλαγών blocks τα οποία προσαρτούν στο blockchain. Η επαλήθευση μιας συναλλαγής επιβεβαιώνει ότι οι συμμετέχοντες έχουν πράγματι στη διάθεσή τους τα bitcoins που εμπλέκονται στη συναλλαγή. Η ιδιοκτησία bitcoins πιστοποιείται χρησιμοποιώντας ένα ζεύγος κρυπτογραφικών κλειδιών, το δημόσιο και το ιδιωτικό κλειδί. Το δημόσιο κλειδί καταγράφεται στο blockchain, ενώ το ιδιωτικό είναι κρυφό και ο ιδιοκτήτης του είναι υπεύθυνος έτσι ώστε να μην διαρρεύσει. Το δημόσιο και το ιδιωτικό κλειδί σχετίζονται

Οποιοσδήποτε λάβει το αρχικό μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα μπορεί να επαληθεύσει μέσω υπολογισμών ότι το digest έχει δημιουργηθεί με το ιδιωτικό κλειδί του αποστολέα χωρίς να γνωρίζει το ιδιωτικό κλειδί του αποστολέα.

6.1.2 Proof of Work

Στο ομότιμο δίκτυο blockchain οι miners ενημερώνονται για νέες συναλλαγές τις οποίες συγκεντρώνουν προκειμένου να δημιουργήσουν ένα νέο block. Ο πρώτος που θα δημιουργήσει και θα επαληθεύσει το block λαμβάνει αμοιβή σε bitcoins. Η επαλήθευση συνίσταται στη δημιουργία ενός hash που να αφορά τα περιεχόμενα των συναλλαγών και το οποίο θα πρέπει να ξεκινά με ένα συγκεκριμένο αριθμό μηδενικών. Η δυσκολία συνίσταται στο ότι δεν υπάρχει τρόπος έτσι ώστε να προβλεφθεί η hash τιμή που επιστρέφει ένα σύνολο δεδομένων. Έτσι, οι miners προσθέτουν στα δεδομένα έναν τυχαίο αριθμό και ευελπιστούν ότι αυτή η προσθήκη θα δώσει την επιθυμητή hash τιμή (που θα ξεκινά με τον απαιτούμενο αριθμό μηδενικών). Ο πρώτος miner που βρίσκει ένα κανοποιητικό hash ανακοινώνει το block στους άλλους miners που το ελέγχουν και εφόσον διαπιστώσουν ότι είναι έγκυρο το προσαρτούν στο blockchain που διατηρούν στους υπολογιστές τους. Η ανταμοιβή των miners προκύπτει από την εξόρυξη νέων bitcoins καθώς και από χρεώσεις συναλλαγών που οι χρήστες εθελοντικά συμπεριλαμβάνουν στις συναλλαγές τους προκειμένου να τους δοθεί προτεραιότητα. Καθώς το mining απαιτεί σημαντική επένδυση σε εξοπλισμό και υψηλές χρεώσεις κατανάλωσης ηλεκτρικού ρεύματος οι miners

έχουν ως κίνητρο τη διατήρηση τηςδημιουργήσει τέτοιες τιμές. Το αντίστοιχο αξιοπιστίας και της ορθής λειτουργίας τουιδιωτικό κλειδί δημιουργείται με τον νομίσματος. Η δε τροποποίηση παρελθόντωναλγόριθμο ECDSA[14]. Πλέον ο χρήστης μπορεί blocks γίνεται ακόμα πιο δύσκολη καθώς όταννα υπογράφει ένα ψηφιακό αρχείο με το δημιουργείται ένα νέο block, περιέχει το hashιδιωτικό του κλειδί και να είναι δυνατή η από το προηγούμενό του στο blockchain.επαλήθευση ότι όντως το υπέγραψε με το Συνεπώς, η τροποποίηση ενός παλιότερουδημόσιο κλειδί του χρήστη. Τελικά, μια block στο blockchain ακυρώνει όλα ταδιεύθυνση bitcoin είναι ένα δημόσιο κλειδί το επόμενά του και θα έπρεπε να διατεθεί απόοποίο υποβάλλεται σε κάποια επιπλέον την αρχή ο υπολογιστικός φόρτοςστάδια επεξεργασίας. Το αποτέλεσμα είναι ότι επαλήθευσης όλων των blocks μέχρι και τοbitcoins που σχετίζονται με μια συγκεκριμένη τελευταίο.

Στην παρούσα φάση η δυσκολία υπολογισμού των κατάλληλων τιμών hashes έχει ρυθμιστεί έτσι ώστε να απαιτούνται περίπου 10 λεπτά για να επιλυθεί ένα μπλοκ που περιέχει 1000 έως 2200 συναλλαγές. Υπολογίζεται δε ότι περίπου 11000 κόμβοι υλοποιούν το πλήρες blockchain πρωτόκολλο, διατηρώντας το σύνολο του blockchain που περιέχει τα στοιχεία όλων των συναλλαγών όπως αυτές έχουν πραγματοποιηθεί από τη 2009 μέχρι σήμερα.

6.1.3 Πορτοφόλια Bitcoin

Ένα πορτοφόλι (wallet) Bitcoin είναι μια απλή εφαρμογή η οποία αναπαριστά τα bitcoins που ο χρήστης του δεν έχει ξοδέψει ακόμα. Δημιουργεί και αποθηκεύει διευθύνσεις που είναι ζεύγη ιδιωτικών και δημόσιων κλειδιών και επιτρέπουν στο χρήστη να χειρίζεται τα bitcoins που του ανήκουν. Ένα Bitcoin πορτοφόλι δεν αποθηκεύει bitcoins. Στην ουσία δεν υφίσταται η έννοια της αποθήκευσης bitcoins καθώς τα bitcoins υφίστανται όταν ανταλλάσσονται μέσω συναλλαγών. Ένα Bitcoin πορτοφόλι χρησιμοποιεί το Bitcoin blockchain έτσι ώστε να εμφανίζει με φιλικό προς το χρήστη τρόπο τον αριθμό από bitcoins που διαθέτει.

Όπως αναφέρθηκε οι διευθύνσεις είναι ζεύγη ιδιωτικών και δημόσιων κλειδιών. Το ιδιωτικό κλειδί μπορεί να είναι οποιοσδήποτε κατάλληλα επιλεγμένος τυχαίος αριθμός και ένα Bitcoin πορτοφόλι είναι σε θέση να διεύθυνση θεωρούνται ότι είναι ιδιοκτησία του κατόχου του αντίστοιχου ιδιωτικού κλειδιού. Αυτό το ιδιωτικό κλειδί χρησιμοποιείται για να υπογράψει συναλλαγές που εμπλέκουν τα bitcoins της διεύθυνσης bitcoin. Μια ιδιαιτερότητα είναι ότι τα bitcoins μιας διεύθυνσης θα πρέπει να διατεθούν στο σύνολό τους όταν συμβαίνει μια συναλλαγή. Άρα, αν χρειαστεί να μεταφερθεί ένας αριθμός από bitcoins από μια ή περισσότερες διευθύνσεις ενός χρήστη σε μια διεύθυνση ενός άλλου χρήστη και υπάρχουν ρέστα στη συναλλαγή τότε το ποσό αυτό μεταφέρεται σε μια νέα διεύθυνση του αρχικού χρήστη.

Οποιοσδήποτε κόμβος δημιουργεί μια συναλλαγή αναλαμβάνει και τη μετάδοσή της στους ομότιμους του κόμβους. Καθένας από αυτούς ελέγχει ότι τα bitcoins δεν έχουν ήδη ξοδευτεί, ότι ανήκουν στον ιδιοκτήτη του δημόσιου κλειδιού που σχετίζεται με τη διεύθυνση του αποστολέα και ότι το ποσό που ξοδεύεται είναι μεγαλύτερο ή ίσο από το ποσό που λαμβάνεται.

6.1.4 Τύποι κόμβων του Bitcoin

Οποιοσδήποτε υπολογιστής μπορεί να είναι ένας κόμβος Bitcoin. Οι πλήρεις κόμβοι (full nodes) θα πρέπει να έχουν επαρκή αποθηκευτικό χώρο και υπολογιστική ισχύ καθώς και υψηλές ταχύτητες επικοινωνίας με το δίκτυο. Οι κόμβοι εξόρυξης (mining nodes) έχουν υψηλότερες υπολογιστικές απαιτήσεις. Το γεγονός αυτό έχει οδηγήσει στη δημιουργία ομάδων που συλλογικά

[14] ECDSA=Elliptic Curve Digital Signing Algorithm

διαθέτουν την υπολογιστική ισχύ των υπολογιστών τους για εξόρυξη. Χρησιμοποιούν δε ειδικά υπολογιστικά συστήματα τύπου ASIC[15] που είναι προσανατολισμένα στο να εκτελούν ταχύτερα τους υπολογισμούς που απαιτεί το Proof Of Work. Άλλη μια κατηγορία κόμβων είναι οι κόμβοι απλής επαλήθευσης πληρωμών (SPV=Simplified Payment Verification) οι οποίοι δεν διατηρούν το πλήρες blockchain αλλά απλά ελέγχουν συγκεκριμένες μόνο συναλλαγές. Οι κόμβοι που εκτελούν λογισμικά πορτοφολιών αποτελούν τυπικές περιπτώσεις αυτού του είδους κόμβων και κατεβάζουν μόνο κεφαλίδες των blocks και όχι τις ίδιες τις συναλλαγές. Τέλος, υπάρχουν και οι κόμβοι πληρωμών (payment nodes) που λειτουργούν ως πύλες προς εξωτερικά συστήματα όπως είναι τα δίκτυα τραπεζών ή πιστωτικών καρτών και χρησιμοποιούνται για την αγορά και πώληση bitcoins διατηρώντας ισοτιμία με συνηθισμένα νομίσματα.

6.1.5 BitcoinCash (BCH)

Το BitcoinCash είναι μια τροποποιημένη έκδοση του βασικού λογισμικού του bitcoin. Το 2017, το project και η κοινότητα του bitcoin διαχωρίστηκε στα δύο. Τα δε σύμβολα που πλέον χρησιμοποιούνται είναι το BTC για το αρχικό Bitcoin και το BCH για το BitcoinCash.

Στην περίπτωση του BCH αυξήθηκε το μέγιστο μέγεθος μπλοκ έτσι ώστε να υποστηρίζει μέγεθος 32MB και με προοπτική το μέγεθος αυτό να αυξηθεί περαιτέρω στο μέλλον. Η αλλαγή στο μέγιστο επιτρεπτό μέγεθος πραγματοποιήθηκε στις 1 Αυγούστου 2017 και οποιοσδήποτε κατείχε bitcoins αυτή τη χρονική στιγμή έγινε ιδιοκτήτης BCH. Το BCH επιτρέπει την εύκολη αποστολή μικρών και μεγάλων χρηματικών ποσών χρεώνοντας μικρές προμήθειες. Ο σχεδιασμός του επιτρέπει τη διενέργεια συναλλαγών με υψηλότερους ρυθμούς σε σχέση με το BTC ενώ δέχεται συνεχείς αναβαθμίσεις έτσι ώστε να αντιμετωπίζονται οι νέες απαιτήσεις που δημιουργούνται.

6.2 Ethereum (ETH)

Το 2013 ο Vitalik Buterin δημιούργησε ένα νέο blockchain με γενικότερη μορφή σε σχέση με το Bitcoin το οποίο ονόμασε Ethereum. Το νόμισμα (token) που χρησιμοποιεί το Ethereum ονομάζεται Ether (ETH) και στη θέση των οικονομικών συναλλαγών που καταγράφονται στο blockchain του Bitcoin υπάρχουν πλέον λιγότερο ή περισσότερο σύνθετα προγράμματα. Οι χρήστες του Ethereum αλληλοεπιδρούν με τα προγράμματα στο blockchain στέλνοντάς τους συναλλαγές εμπλουτισμένες με οδηγίες και τις οποίες επεξεργάζονται οι miners. Η ενσωμάτωση ενός προγράμματος μέσα σε μια συναλλαγή σημαίνει ότι το πρόγραμμα θα μείνει εκεί, διαθέσιμο για όσο εξακολουθεί να υπάρχει το blockchain παρέχοντας στην πράξη διαφάνεια και συνεχή διαθεσιμότητα.

Λίγο μετά την έναρξη λειτουργίας των Distributed Autonomous Organization στο blockchain του Ethereum, ένας χάκερ εκμεταλλεύτηκε ένα σφάλμα σχεδιασμού του και έκλεψε κρυπτονομίσματα ETH αξίας 60 εκατομμυρίων δολαρίων. Η ομάδα που αναπτύσσει το Ethereum αποφάσισε εν μέσω διαμαρτυριών να ακυρώσει τη συναλλαγή έτσι ώστε να επιστρέψει τα χρήματα.

6.2.1 Ethereum Virtual Machine

Το Ethereum δίνει τη δυνατότητα στους χρήστες του να ορίσουν τον τρόπο με τον οποίο θα χρησιμοποιούν το blockchain. Αυτό γίνεται με τα έξυπνα συμβόλαια και τις αποκεντρωμένες εφαρμογές. Την εκτέλεση του κώδικα την αναλαμβάνει το Ethereum Virtual Machine (EVM). Κάθε κόμβος του Ethereum δικτύου τρέχει το EVM και εκτελεί τους ίδιους υπολογισμούς και αποθηκεύει τις ίδιες τιμές. Συνολικά το δίκτυο Ethereum αναφέρεται ως «παγκόσμιος υπολογιστής» και διασφαλίζει την απρόσκοπτη λειτουργία του συστήματος.

[15] ASIC=Application Specific Integrated Circuit

6.2.2 Λογαριασμοί του Ethereum

Υπάρχουν δύο είδη λογαριασμών χρηστών στο Ethereum, οι εξωτερικοί λογαριασμοί (Externally Owned Accounts) και οι λογαριασμοί συμβολαίων. Οι εγγραφές που καταγράφονται στο blockchain αφορούν την κατάσταση των λογαριασμών η οποία μεταβάλλεται από τις συναλλαγές που πραγματοποιούνται. Κάθε λογαριασμός διαθέτει μια διεύθυνση και έναν αριθμό από Ethers που χρησιμοποιούνται ως καύσιμο για την λειτουργία του συστήματος.

6.2.3 Smart Contracts στο Ethereum

Το Ethereum επιτρέπει σε προγραμματιστές να αναπτύσσουν τα δικά τους έξυπνα συμβόλαια ή αυτόνομους πράκτορες (autonomous agents) όπως αλλιώς ονομάζονται. Η γλώσσα προγραμματισμού που μπορεί να χρησιμοποιηθεί είναι "Turing complete" που σημαίνει ότι μπορεί να υποστηρίξει ένα ευρύ σύνολο υπολογιστικών εντολών. Ειδικότερα, τα έξυπνα συμβόλαια μπορούν[16]:

- Να λειτουργήσουν ως «λογαριασμοί πολλαπλών υπογραφών», έτσι ώστε ένα ποσό να δαπανάται μόνο όταν ένα απαιτούμενο ποσοστό ατόμων συμφωνούν.
- Να διαχειρίζονται συμφωνίες μεταξύ χρηστών όπως για παράδειγμα όταν ένας χρήστης αγοράσει μια ασφάλεια από έναν ασφαλιστή.
- Να παρέχουν υπηρεσίες σε άλλα συμβόλαια.
- Να αποθηκεύουν πληροφορίες για μια εφαρμογή όπως για παράδειγμα πληροφορίες που αφορούν τα μέλη μιας υπηρεσίας.

Η εκτέλεση ενός συμβολαίου απαιτεί τέλη συναλλαγής σε ETH που εξαρτάται από την ποσότητα υπολογιστικής ισχύος που απαιτείται. Για να μπορεί να εκτελεστεί ένα έξυπνο συμβόλαιο θα πρέπει ο χρήστης ή ένα άλλο συμβόλαιο να του στείλει ένα μήνυμα και να είναι διαθέσιμη η ποσότητα ETH που χρειάζεται να πληρωθεί ως τέλος συναλλαγής.

6.2.4 Decentralized Applications (DApps)

DApps είναι εφαρμογές που εκτελούνται στο blockchain. Το όνομα αποτελεί σύντμηση των όρων Decentralized (αποκεντρωμένη) και Application (εφαρμογή) και πρόκειται για εφαρμογές που εγκαθίστανται σε ένα κατανεμημένο δίκτυο στο οποίο όλα τα δεδομένα είναι διαφανή και δεν μπορούν να παραποιηθούν. Σε ένα DApp τα δεδομένα αποθηκεύονται σε ένα κατανεμημένο δίκτυο. Οι ψηφιακοί πόροι που αποδίδονται στους χρήστες ανήκουν σε αυτούς και το ίδιο το DApp δεν μπορεί να τους ελέγξει. Επιπλέον, οι κανόνες λειτουργίας του DApp είναι διαφανείς (γνωστοί σε όλους) και δεν μπορούν να αλλάξουν παρά μόνο αν υπάρχει κοινή συναίνεση για αυτό. Προς το παρόν τα περισσότερα παραδείγματα DApps είναι εφαρμογές στοιχημάτων[17] και εφαρμογές συλλογής ψηφιακών τεκμηρίων[18] που δείχνουν ότι τεχνικά μπορούν να λειτουργήσουν εφαρμογές τύπου DApp.

6.2.5 Decentralized Autonomous Organizations (DAO)

DAO είναι μια σύνθετη μορφή έξυπνου συμβολαίου στο οποίο οι κανονισμοί του αποκεντρωμένου οργανισμού βρίσκονται ενσωματωμένοι στον κώδικα του έξυπνου συμβολαίου ενώ παράλληλα ορίζονται και κανόνες διαχείρισης του token που χρησιμοποιείται στις συναλλαγές. Το bitcoin θεωρείται ως το πρώτο DAO.

6.3 Εναλλακτικά κρυπτονομίσματα (altcoins)

Πέρα από το Bitcoin και το Ethereum υπάρχουν εκατοντάδες άλλα ψηφιακά νομίσματα που συλλογικά αναφέρονται ως

[16] https://www.coindesk.com/information/ethereum-smart-contracts-work

[17] https://www.fairhouse.io/

[18] https://www.cryptokitties.co/

altcoins. Στη συνέχεια γίνεται αναφορά σε ορισμένα από τα πλέον διαδεδομένα altcoins.

6.3.1 Litecoin (LTC)

Το Litecoin εμφανίστηκε το 2011 ως αποτέλεσμα της εργασίας του Charlie Lee, ενός πρώην υπαλλήλου της Google, ο οποίος οραματίστηκε μια ταχύτερη έκδοση του bitcoin που θα μπορούσε να χρησιμοποιηθεί για καθημερινές συναλλαγές μικρής αξίας. Προσφέρει ταχύτερους χρόνους επιβεβαίωσης συναλλαγών σε σχέση με το bitcoin και χρησιμοποιεί ως PoW μια διαδικασία στην οποία έχει αποδοθεί το όνομα "scrypt". Η διαδικασία scrypt έχει σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να καθιστά δυσκολότερη τη χρήση εξειδικευμένων υπολογιστικών συστημάτων που θα αναλάμβαναν την εξόρυξη και θα έδιναν συγκριτικό πλεονέκτημα στους κατόχους τους. Συνεπώς, στοχεύει στον περαιτέρω εκδημοκρατισμό του δικτύου.

6.3.2 Zcash (ZEC)

Το Zcash εμφανίστηκε το 2016 και προσφέρει επιπλέον ασφάλεια και ιδιωτικότητα στις συναλλαγές που καταγράφονται στο blockchain του. Τα ευαίσθητα δεδομένα των συναλλαγών μπορούν να κρυπτογραφηθούν χρησιμοποιώντας τον αλγόριθμο zk-SNARK. Πρόκειται για έναν αλγόριθμο που υλοποιεί ZKP (απόδειξη μηδενικής γνώσης) πάνω στο blockchain.

6.3.3 Dash (DASH)

Το Dash αναπτύχθηκε το 2014 από τον Evan Duffield και αναπτύχθηκε πάνω στον αρχικό κώδικα του bitcoin. Η αρχική του ονομασία ήταν Darkcoin και προσέφερε μεγαλύτερη ανωνυμία σε σχέση με το bitcoin καθώς οι συναλλαγές που καταγράφονται στο Dash δίκτυο είναι ακόμα δυσκολότερο να ανιχνευθούν. Η τεχνολογία InstantX του Dash μπορεί να ολοκληρώσει μια συναλλαγή κατά μέσο όρο σε 4 δευτερόλεπτα (ο αντίστοιχος χρόνος για το bitcoin είναι 15 λεπτά).

6.3.4 Monero (XMR)

Το Monero είναι ένα κρυπτονόμισμα που είναι προσανατολισμένο στην ιδιωτικότητα των συναλλαγών. Μόνο οι συμμετέχοντες σε μια συναλλαγή έχουν πρόσβαση στις διευθύνσεις των συναλλασσόμενων μερών και την αξία της συναλλαγής, σε αντίθεση με το bitcoin που οι πληροφορίες αυτές είναι δημόσια διαθέσιμες. Λόγω των χαρακτηριστικών απόκρυψης των στοιχείων των συναλλαγών που διαθέτει αποτελεί σύνηθες νόμισμα συναλλαγών σε αγορές του σκοτεινού διαδικτύου (darknet[19]).

6.3.5 Ripple (XRP)

Το Ripple έχει σήμερα (Απρίλιος 2019) την τρίτη μεγαλύτερη κεφαλαιοποίηση αγοράς μετά το Bitcoin και το Ethereum. Είναι προσανατολισμένο προς μεγάλες επιχειρήσεις παρά προς μεμονωμένους χρήστες. Παρέχει υπηρεσίες χρηματοοικονομικού διακανονισμού σε τράπεζες επιτρέποντας απευθείας συναλλαγές που υπερβαίνουν τα εθνικά σύνορα χωρίς χρονοβόρες καθυστερήσεις. Μεγάλοι χρηματοοικονομικοί και άλλοι οργανισμοί (π.χ. Bank of America, Santander, UniCredit, Royal Bank of Canada κ.α.) υποστηρίζουν ενεργά τη συγκεκριμένη τεχνολογία και η εταιρεία Ripple Labs που την αναπτύσσει έχει λάβει σημαντική χρηματοδότηση. Το πρωτόκολλο Ripple (RXTP) και το δίκτυο πληρωμών της εταιρείας ώθησε το MIT Technology Review στο τεύχος που εκδόθηκε τον Φεβρουάριο του 2014 στο να συμπεριλάβει την Ripple Labs στις 50 «εξυπνότερες» εταιρείες της χρονιάς. Το κρυπτονόμισμα που χρησιμοποιεί έχει την επωνυμία XRP ενώ το blockchain διατηρείται σε ένα σύνολο από διακομιστές που μπορούν να ανήκουν σε άμεσα ενδιαφερόμενα μέλη (π.χ. τράπεζες, ελεγκτικούς οργανισμούς) αλλά και σε οποιονδήποτε. Το δε ενεργειακό αποτύπωμα των διακομιστών του είναι ιδιαίτερα χαμηλό. Οι συναλλαγές επιβεβαιώνονται από τους διακομιστές σε

[19] https://el.wikipedia.org/wiki/Dark_Web

ελάχιστο χρόνο, είναι μη αναστρέψιμες και δεν απαιτούνται επιπλέον χρεώσεις.

6.3.6 Stellar (XLM)

Το Stellar παρέχει ταχύτατες και φθηνές διασυνοριακές υπηρεσίες πληρωμών παρόμοια με το Ripple, αλλά στοχεύει σε μεμονωμένους χρήστες. Υποστηρίζεται από μεγάλες εταιρείες τεχνολογίας όπως η IBM. Οι διακομιστές στους οποίους διατηρείται το blockchain του Stellar δεν έχουν σημαντικές απαιτήσεις κατανάλωσης ενέργειας καθώς όπως και στο Ripple δεν χρησιμοποιείται PoW. Το δε κρυπτονόμισμα που χρησιμοποιεί ονομάζεται XLM.

6.3.7 EOS

Το EOS στοχεύει στη βελτίωση ορισμένων ατελειών του Ethereum. Επιτρέπει την ανάπτυξη dApp χωρίς γνώση της γλώσσας προγραμματισμού έξυπνων συμβολαίων Solidity καθώς και γενικότερα προγραμματιστικών γνώσεων. Επιπλέον, είναι ταχύτερο (1,5 δευτερόλεπτο έναντι 6 λεπτών του Ethereum για την επιβεβαίωση συναλλαγών) και μπορεί να κλιμακωθεί σε μεγαλύτερο βαθμό από το Ethereum. Δεν απαιτεί από τους χρήστες να πληρώνουν “gas” για τη χρήση του καθώς είναι δωρεάν και μπορεί να διαχειριστεί μέχρι και 50.000 συναλλαγές το δευτερόλεπτο. Δεν ακολουθεί διαδικασία εξόρυξης των νέων μπλοκ αλλά οι παραγωγοί μπλοκ ψηφίζονται από την κοινότητα του EOS.

6.4 ICO

ICO (Initial Coin Offering), αρχική προσφορά νομισμάτων, είναι ένας μηχανισμός χρηματοδότησης για επιχειρηματικές ιδέες οι οποίες στηρίζονται στο blockchain. Η βασική ιδέα είναι ότι δημιουργείται ένα νέο νόμισμα που απαιτείται έτσι ώστε να επιτρέπεται η χρήση της εφαρμογής μέσω της οποίας θα υλοποιείται η επιχειρηματική ιδέα. Ένας αριθμός αυτών των νομισμάτων διατίθενται προς πώληση πριν την εκκίνηση της εφαρμογής έτσι ώστε οποιοσδήποτε ενδιαφερόμενος να μπορεί να τα αποκτήσει.

7 Έξυπνα συμβόλαια

7.1 Τι είναι ένα έξυπνο συμβόλαιο;

Ένα έξυπνο συμβόλαιο είναι ένα πρόγραμμα το οποίο εκτελείται πάνω σε μια υποδομή blockchain και περιέχει κανόνες που οι συμμετέχοντες έχουν συμφωνήσει να τηρούν στις μεταξύ τους αλληλεπιδράσεις. Όταν οι προκαθορισμένες προϋποθέσεις ενός έξυπνου συμβολαίου ικανοποιηθούν, το συμβόλαιο ενεργοποιείται αυτόματα. Αυτό έχει ως αποτέλεσμα την εκτέλεση των ενεργειών που προδιαγράφει το συμβόλαιο και οι οποίες έχουν να κάνουν με την κατανομή ψηφιακών πόρων μεταξύ των εμπλεκομένων μελών βάσει ενός καταγεγραμμένου αλγορίθμου και συμπληρωματικών δεδομένων που καθορίζουν τη συμπεριφορά του συμβολαίου τη στιγμή που ενεργοποιείται.

Ο όρος έξυπνο συμβόλαιο είναι μάλλον ατυχής καθώς δεν πρόκειται ούτε για κάτι έξυπνο ούτε για συμβόλαιο[20]. Ο λόγος για τον οποίο δεν μπορεί να θεωρηθεί έξυπνο είναι διότι απλά αποτελεί αποτύπωση της «εξυπνάδας» του προγραμματιστή του δεδομένης της γνωστής σε αυτόν πληροφορίας τη στιγμή που το συντάσσει. Συνεπώς, δεν έχει τη δυνατότητα προσαρμογής σε νέες ή πρωτόγνωρες καταστάσεις που αποτελεί βασικό συστατικό της έξυπνης (νοήμονος) συμπεριφοράς. Από την άλλη μεριά αν και χρησιμοποιείται ο όρος «συμβόλαιο» δεν θα πρέπει να συγχέεται με την έννοια του νομικού συμβολαίου που γίνεται αποδεκτό από δικαστήρια ή εποπτικές αρχές κρατών. Ωστόσο, δεν είναι απίθανο στο μέλλον να υπάρξει ομογενοποίηση έξυπνων συμβολαίων και συμβολαίων με νομική ισχύ καθώς η τεχνολογία των έξυπνων συμβολαίων θα ωριμάζει.

Στον

[20] https://www.forbes.com/sites/davidblack/2019/02/04/blockchain-smart-contracts-arent-smart-and-arent-contracts

Κώδικας 1 παρουσιάζεται ο κώδικα ενός έξυπνου συμβολαίου για το Ethereum[21]. Στο Ethereum η γλώσσα προγραμματισμού έξυπνων συμβολαίων είναι η solidity που παρουσιάζει ομοιότητες με την ιδιαίτερα διαδεδομένη γλώσσα προγραμματισμού javascript.

```
pragma solidity ^0.4.22;

contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    // Ensure that `msg.value` is an even number.
    // Division will truncate if it is an odd number.
    // Check via multiplication that it wasn't an odd number.
    constructor() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value, "Value has to be even.");
    }

    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(
            msg.sender == buyer,
            "Only buyer can call this."
        );
        _;
    }

    modifier onlySeller() {
        require(
            msg.sender == seller,
            "Only seller can call this."
        );
        _;
    }

    modifier inState(State _state) {
        require(
            state == _state,
            "Invalid state."
        );
        _;
    }

    event Aborted();
    event PurchaseConfirmed();
    event ItemReceived();

    /// Abort the purchase and reclaim the ether.
    /// Can only be called by the seller before
    /// the contract is locked.
    function abort()
        public
        onlySeller
        inState(State.Created)
    {
        emit Aborted();
        state = State.Inactive;
        seller.transfer(address(this).balance);
    }

    /// Confirm the purchase as buyer.
    /// Transaction has to include `2 * value` ether.
    /// The ether will be locked until confirmReceived
    /// is called.
    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }

    /// Confirm that you (the buyer) received the item.
    /// This will release the locked ether.
    function confirmReceived()
        public
        onlyBuyer
        inState(State.Locked)
    {
        emit ItemReceived();
        // It is important to change the state first because
        // otherwise, the contracts called using `send` below
        // can call in again here.
        state = State.Inactive;

        // NOTE: This actually allows both the buyer and the seller to
        // block the refund - the withdraw pattern should be used.

        buyer.transfer(value);
        seller.transfer(address(this).balance);
    }
}
```

Κώδικας 1. Παράδειγμα έξυπνου συμβολαίου (ασφαλής απομακρυσμένη αγορά[22])

7.2 Πλεονεκτήματα έξυπνων συμβολαίων

Το κύριο πλεονέκτημα των έξυπνων συμβολαίων είναι ότι μειώνουν δραματικά τα κόστη συναλλαγών. Ένα έξυπνο συμβόλαιο ορίζει τα δικαιώματα και τις υποχρεώσεις που τα συμμετέχοντα μέλη συμφωνούν να τηρούν. Ο έλεγχος τήρησης των υποχρεώσεων και η επιβολή του δικαιώματος που αποκτά κάθε μέλος δια του συμβολαίου διεκπεραιώνονται από ένα δίκτυο υπολογιστών τη στιγμή που οι προϋποθέσεις ικανοποιούνται. Με αυτό τον τρόπο δίνεται η δυνατότητα σύναψης συμβολαίων με μέλη για τα οποία δεν υπάρχουν πληροφορίες πρότερης φερεγγυότητας καθώς και η πραγματοποίηση συναλλαγών που εμπλέκουν ποσά που δεν θα δικαιολογούσαν το κόστος και φόρτο σύναψης συμφωνιών εάν επρόκειτο να προχωρήσουν με τον παραδοσιακό τρόπο. Τα έξυπνα συμβόλαια λειτουργούν συνεχώς και δεν επιβάλουν περιορισμούς διαθεσιμότητας που σχετίζονται με χρόνο ή τοποθεσία.

Τα έξυπνα συμβόλαια ελέγχουν σε πραγματικό χρόνο τη συμμόρφωση των μελών. Προκειμένου να λάβουν πληροφορίες από τον «εξωτερικό» κόσμο ενδέχεται να χρειάζονται πηγές εξωτερικής πληροφόρησης που αναλαμβάνουν να προμηθεύσουν τις απαιτούμενες

[21] https://blockgeeks.com/guides/smart-contracts/
[22] https://solidity.readthedocs.io/en/v0.4.24/solidity-by-example.html#safe-remote-purchase

πληροφορίες (π.χ. καιρικές καταστάσεις). Τα έξυπνα συμβόλαια είναι αυτό-επαληθευόμενα, αυτό-εκτελέσιμα και μη παραβιάσιμα. Τυπικές περιπτώσεις χρήσης τους είναι περιπτώσεις στις οποίες τα μέλη που επιθυμούν να συνάψουν συμβόλαιο δεν είναι γνωστά μεταξύ τους και δεν εμπιστεύονται κατ' ανάγκη το ένα το άλλο. Μπορούν να παρακάμψουν διαμεσολαβητές και μέσω του blockchain να προσφέρουν την απαιτούμενη ασφάλεια.

Μια σύνοψη των πλεονεκτημάτων των έξυπνων συμβολαίων έναντι των παραδοσιακών συμβολαίων παρουσιάζεται στον Πίνακας 1.

Παραδοσιακά συμβόλαια	Έξυπνα συμβόλαια
1-3 ημέρες	Λεπτά
Μη αυτοματοποιημένα εμβάσματα	Αυτοματοποιημένα εμβάσματα
Απαραίτητη χρηματική εγγύηση	Η χρηματική εγγύηση μπορεί να μην είναι απαραίτητη
Ακριβά	Φθηνά
Απαίτηση φυσικής παρουσίας	Μη απαίτηση φυσικής παρουσίας (ψηφιακές υπογραφές)
Υποχρεωτική παρουσία δικηγόρων	Μη υποχρεωτική παρουσία δικηγόρων

Πίνακας 1. Πλεονεκτήματα έξυπνων συμβολαίων

7.3 Κατηγορίες έξυπνων συμβολαίων

Συχνά διατυπώνεται η άποψη ότι τα έξυπνα συμβόλαια μέσω του blockchain θα προκαλέσουν σημαντικές αλλαγές ή και πλήρη αναδιάταξη επιχειρηματικών χώρων [8], [9]. Εικάζεται μάλιστα η χρήση τους σε ευρεία γκάμα εφαρμογών από απλές μέχρι αρκετά σύνθετες (Εικόνα 16). Περιπτώσεις χρήσης που αναφέρονται είναι η τραπεζική, οι ασφάλειες, η ενέργεια, η ηλεκτρονική διακυβέρνηση, οι επικοινωνίες, η βιομηχανία θεάματος, οι τέχνες, η εκπαίδευση και άλλες.

Εικόνα 16. Έξυπνα συμβόλαια (απλά προς σύνθετα) Πηγή: PricewaterhouseCoopers

Σχετικά απλές περιπτώσεις χρήσης θεωρούνται οι υπηρεσίες χρονικής σφράγισης (π.χ. για πνευματικά δικαιώματα) και τα αρχεία κυβερνητικών και άλλων υπηρεσιών (π.χ. τίτλοι ιδιοκτησίας, πιστοποιητικά γέννησης, βεβαιώσεις αποφοίτησης - πτυχία). Από την άλλη

μεριά οι αποκεντρωμένοι αυτόνομοι οργανισμοί (DAOs =Distributed Autonomous Organizations) θεωρούνται ως τα πλέον σύνθετα παραδείγματα χρήσης των έξυπνων συμβολαίων.

7.3.1 Ένα παράδειγμα έξυπνου συμβολαίου

Τα έξυπνα συμβόλαια είναι προγράμματα τα οποία βρίσκονται στο blockchain και τα οποία παρέχουν υπηρεσίες οι οποίες χρεώνονται χρησιμοποιώντας κρυπτονομίσματα. Ένα blockchain δεν μπορεί να αποθηκεύσει μεγάλες ποσότητες δεδομένων ούτε να παρέχει απευθείας απαντήσεις για την κατάσταση του φυσικού κόσμου. Συνεπώς θα πρέπει να χρησιμοποιεί υπηρεσίες που υφίστανται εκτός του blockchain. Στη συνέχεια παρουσιάζεται ένα παράδειγμα του περιγράφει το πως θα μπορούσε να λειτουργεί ένα έξυπνο συμβόλαιο που παρέχει αυτόματη ασφάλιση πτήσεων [10]. Στο παράδειγμα αυτό χρησιμοποιείται μια υπηρεσία “oracle” (μαντείο), εκτός του blockchain, έτσι ώστε να ανακαλούνται δεδομένα για τις καθυστερήσεις πτήσεων.

Βήμα 1

Ένας πελάτης πρόκειται να πραγματοποιήσει μια πτήση και επιθυμεί να προσθέσει ταξιδιωτική ασφάλιση σε αυτή. Ο πελάτης στέλνει τις πληροφορίες της πτήσης του και ethers σε ένα έξυπνο συμβόλαιο.

Βήμα 2

Το έξυπνο συμβόλαιο ζητά από την υπηρεσία oracle να επιβεβαιώσει τα δεδομένα της πτήσης και να συγκεντρώσει πληροφορίες σχετικά με τη διαδρομή της πτήσης.

Βήμα 3

Το έξυπνο κεφάλαιο ελέγχει με βάση τα στοιχεία που έλαβε εάν το ποσό επαρκεί. Αν αυτό ισχύει τότε λαμβάνει από την υπηρεσία oracle δεδομένα για την κατάσταση της πτήσης.

Βήμα 4

Η υπηρεσία oracle χρησιμοποιεί real time πληροφορίες[23] έτσι ώστε να αναφέρει την κατάσταση της πτήσης στο έξυπνο συμβόλαιο.

Βήμα 5

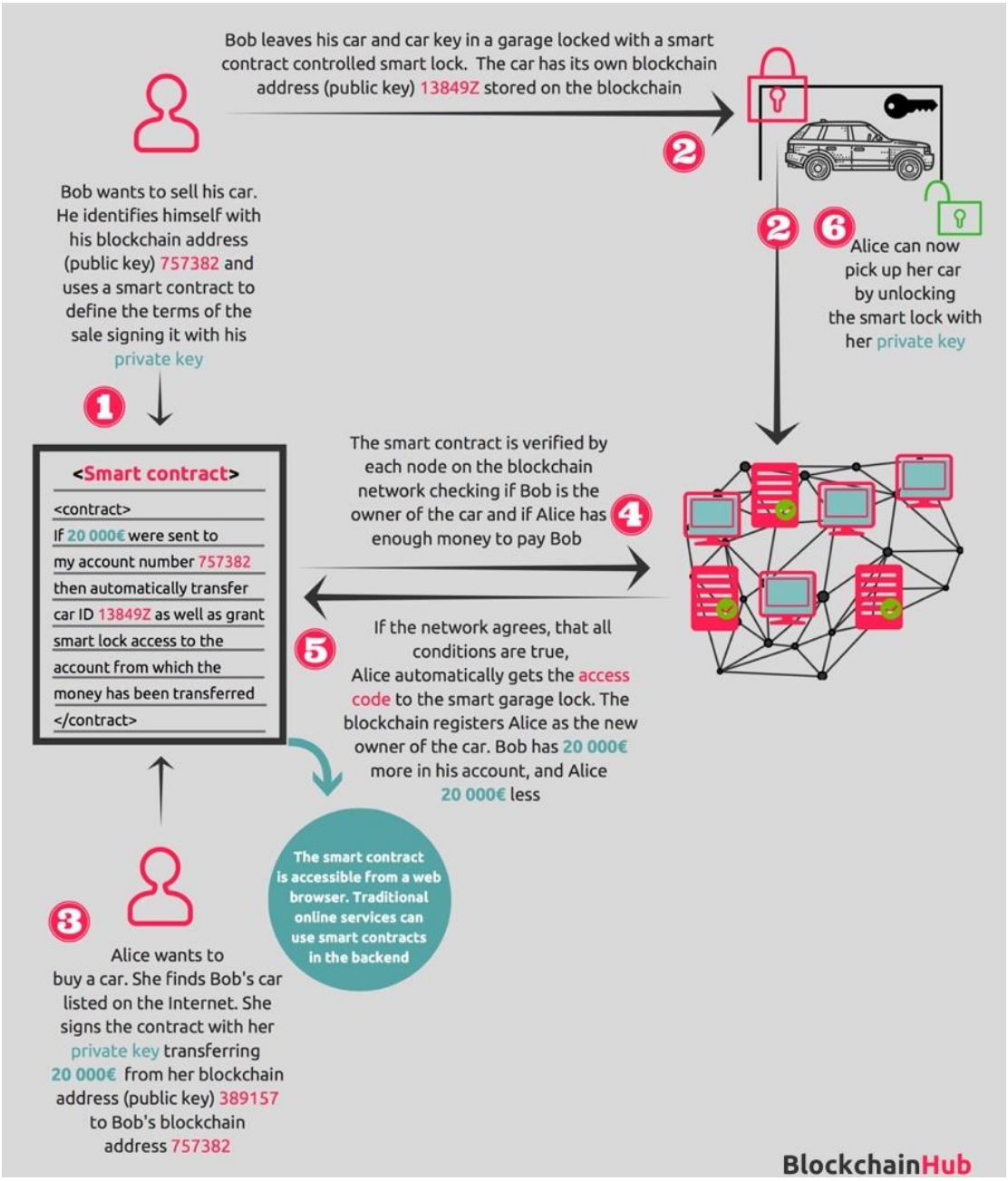
Αν η πτήση καθυστερήσει το έξυπνο συμβόλαιο αποζημιώνει τον επιβάτη ενώ αν η πτήση δεν καθυστερήσει το συμβόλαιο πληρώνεται.

7.3.2 Ένα δεύτερο παράδειγμα έξυπνου συμβολαίου

Ως δεύτερο παράδειγμα θα παρουσιαστεί η περίπτωση αγοράς και πώλησης ενός αυτοκινήτου[24]. Παραδοσιακά, αν ο αγοραστής Α θέλει να αγοράσει ένα αυτοκίνητο από τον Β, ένας αριθμός από διαμεσολαβητές-μεσάζοντες θα πρέπει να παρεμβληθούν έτσι ώστε να διασφαλίσουν και να επαληθεύσουν την αγοραπωλησία. Διαμεσολαβητές στη συγκεκριμένη περίπτωση είναι το Υπουργείο Μεταφορών, μια ασφαλιστική εταιρεία και πιθανώς άλλοι. Η διαδικασία είναι πολύπλοκη και με σημαντικό κόστος.

[23] https://www.flightradar24.com
[24] https://blockchainhub.net/smart-contracts/

Θεωρώντας ότι όλοι οι εμπλεκόμενοι έχουν αποφασίσει την υιοθέτηση μιας λύσης blockchain η επαλήθευση της συναλλαγής θα γίνει πλέον από τους κόμβους του δικτύου blockchain μέσω του οποίου θα ελεγχθεί ότι ο Β έχει στην ιδιοκτησία του το αυτοκίνητο και ο Α διαθέτει το ποσό που θα του επιτρέψει την αγορά. Αν και οι δυο συνθήκες επαληθευτούν από το δίκτυο, ο Α δέχεται τον ειδικό κωδικό που θα του επιτρέψει να έχει πρόσβαση σε μια έξυπνη κλειδαριά που κρατά προστατευμένο σε γκαράζ το αυτοκίνητο, ο Α καταγράφεται ως νέος ιδιοκτήτης του αυτοκινήτου, ο Β λαμβάνει το αντίτιμο της συναλλαγής στο λογαριασμό του και το ποσό αφαιρείται από το λογαριασμό του Α. Η διαδικασία ενεργοποίησης του έξυπνου συμβολαίου παρουσιάζεται στην Εικόνα 17 η οποία έχει ληφθεί από την ιστοσελίδα blockchainhub.net.



Εικόνα 17. Αγορά αυτοκινήτου – έξυπνο συμβόλαιο

8 Περιπτώσεις χρήσης του blockchain

Το blockchain μπορεί να χρησιμοποιηθεί σε πληθώρα εφαρμογών χωρίς να απαιτείται άμεση σύνδεση με χρηματοοικονομικά. Η διαπίστωση αυτή έγινε σχεδόν ταυτόχρονα με την κυκλοφορία του bitcoin που αποτέλεσε την πρώτη επιτυχημένη εφαρμογή της ιδέας ενός κατανεμημένου καθολικού που διατηρείται σε συνεπή κατάσταση από ένα μεγάλο αριθμό ομότιμων συμμετεχόντων μέρος των οποίων μπορεί να λειτουργούν εχθρικά έναντι των άλλων μελών. Το blockchain μπορεί να χρησιμοποιηθεί ως μια αποθήκη δεδομένων γενικής φύσεως για τα οποία ισχύει ότι ήδη καταγεγραμμένα δεδομένα δεν μπορούν να τροποποιηθούν ενώ επιτρέπεται η προσάρτηση νέων δεδομένων στα οποία εφόσον απαιτείται καταγράφεται η χρονική στιγμή δημιουργίας τους. Συνεπώς, το blockchain μπορεί να λειτουργήσει:

- Ως μητρώο αντικειμένων που πρέπει να είναι μοναδικά. Παραδείγματα αποτελούν οι άδειες χρήσης, οι πατέντες, οι επωνυμίες επιχειρήσεων, τα πρόστιμα, οι εγγραφές παραπόνων και οι καταδικαστικές αποφάσεις.
- Ως μητρώο γεγονότων με καταγραφή της χρονικής στιγμής στην οποία προσαρτώνται οι εγγραφές. Σχετικές εφαρμογές είναι η παρακολούθηση πληρωμών, η παρακολούθηση διαδικασιών παράδοσης.
- Ως μητρώο ακολουθίας γεγονότων που πρέπει να συμβούν με συγκεκριμένη σειρά όπως είναι η διεκπεραίωση αιτήσεων από την έναρξη μέχρι την ολοκλήρωσή τους.
- Ως μητρώο ταυτότητας για άτομα, ζώα και αγαθά.
- Ως μητρώο πνευματικής κυριότητας. Σχετικές εφαρμογές αποτελούν η παρακολούθηση αλλαγών σε έγγραφα, η ηλεκτρονική δημοσίευση και η διάθεση ψηφιακού περιεχομένου.
- Ως μητρώο ιδιοκτησίας στο οποίο καταγράφεται η ιδιοκτησία κινητών και ακινήτων πόρων.

Ενδιαφέρον για την τεχνολογία blockchain έχουν δείξει, μεταξύ άλλων, ο τραπεζικός τομέας, ο τομέας των μεταφορών, ο τομέας της εκπαίδευσης, ο φαρμακευτικός τομέας κ.α. Ένα πρόβλημα στο οποίο ενδεχόμενα το blockchain μπορεί να προσφέρει λύση είναι η μερική και συχνά ατελής ή ασυνεπής καταγραφή εγγραφών.

Σε πολλές εφαρμογές το θέμα της ιδιωτικότητας είναι εξαιρετικά σημαντικό. Ένα δημόσια διαθέσιμο blockchain όπως του Bitcoin ακόμα και αν δεν περιέχει τις πραγματικές ταυτότητες των συμμετεχόντων είναι ευάλωτο σε ανίχνευση και ανάλυση προτύπων που μπορεί να οδηγήσει σε αποκάλυψη ταυτοτήτων. Το γεγονός αυτό σε συνδυασμό με το σχετικά χαμηλό ρυθμό συναλλαγών (λόγω του PoW) που είναι σε θέση να διεκπεραιώσει ένα δημόσιο blockchain έχει οδηγήσει στην προσαρμογή της τεχνολογίας blockchain έτσι ώστε πλέον να εξυπηρετεί καλύτερα συγκεκριμένα είδη εφαρμογών. Αυτό συμβαίνει μέσω των ιδιωτικών blockchains στα οποία οι συμμετέχοντες είναι γνωστοί και συνεπώς θέματα που έχουν να κάνουν με τη διατήρηση της ανωνυμίας, την αντιμετώπιση της κακόβουλης συμπεριφοράς και τη διάθεση της αμοιβής για την επαλήθευση των συναλλαγών αποκτούν δευτερεύουσα σημασία. Αντίθετα, στα ιδιωτικά blockchains έμφαση δίνεται στο ρυθμό διεκπεραίωσης των συναλλαγών και στη λειτουργικότητα της εφαρμογής.

8.1 Χρηματοοικονομικά

Οι χρηματοοικονομικοί οργανισμοί ήταν από τους πρώτους που έδειξαν ενδιαφέρον για την τεχνολογία blockchain. Ο χώρος των χρηματοοικονομικών εξάλλου βρίσκεται σε συνεχή αναζήτηση επιτυχημένων καινοτομιών που θα δώσουν έστω και για λίγο, πριν υιοθετηθούν καθολικά και από τους ανταγωνιστές, συγκριτικό πλεονέκτημα. Η ανάπτυξη και η εφαρμογή της τεχνολογίας στα χρηματοοικονομικά είναι γνωστή ως Fintech (Financial Technology) και αγγίζει την καθημερινότητα των συναλλαγών με υπηρεσίες του δημοσίου, με τράπεζες και με άλλους χρηματοοικονομικούς οργανισμούς.

Ο αριθμός των μεσαζόντων που απαιτούνται για την ολοκλήρωση πολλών χρηματοοικονομικών συναλλαγών είναι υψηλός. Για παράδειγμα, απαιτούνται τουλάχιστον πέντε μεσάζοντες για την επεξεργασία μιας απλής συναλλαγής με πιστωτική κάρτα.

8.2 Αγοραπωλησίες ακινήτων

Ορισμένα από τα προβλήματα που αντιμετωπίζει η αγορά ακινήτων σήμερα είναι η περιορισμένη πρόσβαση πελατών στην προσφορά ακινήτων, οι χρονοβόρες διαδικασίες για την ολοκλήρωση αγοραπωλησιών, τα λάθη στις καταγραφές τίτλων ιδιοκτησίας, τα υψηλά τέλη αγοραπωλησιών και τα περιστατικά απάτης. Ορισμένες καινοτομίες που αναμένεται να επιφέρει η τεχνολογία blockchain στο συγκεκριμένο χώρο είναι οι ακόλουθες[25]:

- **Tokenization (τμηματική πώληση/αγορά ιδιοκτησίας)**: Χρησιμοποιώντας κρυπτονομίσματα καθίσταται τεχνικά δυνατό να «σπάσει» μια ιδιοκτησία σε μερίσματα που αποθηκεύονται στο blockchain. Με αυτό τον τρόπο οι ιδιοκτήτες έχουν τη δυνατότητα να πουλήσουν ένα μέρος μόνο της ιδιοκτησίας τους. Το εύρος των πιθανών αγοραστών γίνεται μεγαλύτερο και παύουν να υπάρχουν γεωγραφικοί περιορισμοί. Επενδυτές που διαθέτουν μικρότερα κεφάλαια μπορούν να επενδύσουν σε ιδιοκτησίες μεγάλης συνολικής αξίας. Ως παράδειγμα μπορεί να αναφερθεί η περίπτωση της Templus Markets που έδωσε τη δυνατότητα σε επενδυτές, με τη μέθοδο του ψηφιακού tokenization, να επενδύσουν στο ξενοδοχείο St. Regis[26] στο Άσπεν διαθέτοντας ποσά που ξεκινούσαν από $10.000 ενώ η συνολική αξία του ξενοδοχείου υπολογίζονταν στα $18.000.000.
- **Έξυπνα συμβόλαια**: Η τρέχουσα κατάσταση στις αγοραπωλησίες ακινήτων εμπλέκει πολλούς μεσάζοντες ενώ τα έξυπνα συμβόλαια απαιτούν συμμετοχή μόνο του πωλητή και του αγοραστή. Ολοκληρώνονται σε πολύ συντομότερο χρόνο και είναι λιγότερο ευάλωτα σε απόπειρες απάτης. Οι πλήρεις πληροφορίες της αγοραπωλησίας βρίσκονται καταγεγραμμένες ψηφιακά και κρυπτογραφημένες έτσι ώστε να μπορούν να αναγνωστούν μόνο από όσους έχουν δικαίωμα. Με αυτόματο τρόπο όταν ικανοποιηθούν όλοι οι όροι του κάθε συμβολαίου πραγματοποιείται η αλλαγή ιδιοκτησίας και η αποπληρωμή.
- **Τίτλοι ιδιοκτησίας**: Οι τίτλοι ιδιοκτησίας στην παρούσα φάση διατηρούνται σε υποθηκοφυλακεία ή σε διάφορες διάσπαρτες ηλεκτρονικές εφαρμογές. Για παράδειγμα στην Ελλάδα κάθε Δήμος έχει το υποθηκοφυλακείο του και τα τελευταία χρόνια γίνεται προσπάθεια έτσι ώστε όλη η σχετική πληροφορία να μεταφερθεί στην

[25] https://www.forbes.com/sites/forbesrealestatecouncil/2018/11/15/three-ways-blockchain-technology-will-revolutionize-real-estate-in-2019/#34574c706d20

[26] https://www.aspentimes.com/news/local/in-18-million-deal-nearly-one-fifth-of-st-regis-aspen-sells-through-digital-tokens/

εφαρμογή του κτηματολογίου[27]. Ωστόσο, αν όλη η πληροφορία ιδιοκτησιών ήταν αποκεντρωμένη σε blockchain θα υπήρχε η δυνατότητα να εξοικονομηθεί ένα τεράστιο χρηματικό ποσό. Επιπλέον, θα μπορούσε να καταγράφεται στο blockchain ιστορικό βλαβών, προσθηκών και μετατροπών σε κάθε ιδιοκτησία έτσι ώστε ο πιθανός αγοραστής να γνωρίζει πλήρως τα στοιχεία της ιδιοκτησίας για την οποία ενδιαφέρεται. Η ποσότητα της πληροφορίας που θα πρέπει να καταγράφεται στο blockchain είναι τεράστια και αυτό αποτελεί μια πρόκληση που θα πρέπει να αντιμετωπιστεί. Βέβαια, η μεγαλύτερη πρόκληση είναι η αποδοχή της συγκεκριμένης τεχνολογίας από τους φορείς της πολιτείας.

8.3 Ηλεκτρονική διακυβέρνηση

Οι κυβερνήσεις ανά τον κόσμο διαθέτουν πληθώρα πόρων προκειμένου να διατηρούν αρχεία στα οποία καταγράφεται η ταυτότητα ατόμων και η ιδιοκτησία περιουσιακών στοιχείων. Η εγκυρότητα των στοιχείων μπορεί να τίθεται υπό αμφισβήτηση λόγω παραχάραξης τεκμηρίων. Επιπλέον, εκατομμύρια άνθρωποι δεν διαθέτουν στοιχεία ταυτότητας (π.χ. πρόσφυγες) ή έχουν παραχαράξει τα έγγραφα ταυτοποίησής τους. Στα φτωχότερα μέρη του πλανήτη η πρόσβαση σε βασικές υπηρεσίες (π.χ. τραπεζική) μπορεί να προσκρούει στην αδυναμία σημαντικής μερίδας του πληθυσμού να παρουσιάσει μόνιμη διεύθυνση κατοικίας και λογαριασμούς ρεύματος ή νερού που να έχουν εκδοθεί στο όνομά τους. Κυβερνήσεις και οργανισμοί μπορούν να υιοθετήσουν μια λύση blockchain εκδίδοντας για παράδειγμα ψηφιακά πιστοποιητικά γέννησης που δεν μπορούν να παραχαραχθούν και είναι προσβάσιμα από οποιονδήποτε έχει την απαιτούμενη διαβάθμιση πρόσβασης. Με αυτό τον τρόπο μπορεί να επιτευχθεί μείωση κόστους και χρόνου για την επαλήθευση ταυτοτήτων ατόμων και ιδιοκτησιών και καταπολέμηση του φαινομένου της εμπορίας ανθρώπων (human trafficking).

8.4 Υπηρεσίες ταυτοποίησης

Συχνά, αποκτούν δημοσιότητα περιπτώσεις ψηφιακής παραβίασης ιδιωτικότητας που συμβαίνουν λόγω του ότι μεγάλες ή μικρότερες επιχειρήσεις αποτυγχάνουν να διαθέσουν στους πελάτες τους ασφαλή πληροφοριακά συστήματα, διατηρώντας ελαττωματικά λογισμικά ή παρωχημένα, ευπαθή συστήματα. Η ιδέα της ύπαρξης ενός blockchain στο οποίο θα υπάρχουν ψηφιακά πιστοποιητικά που θα έχουν εκδοθεί από αξιόπιστους και γνωστούς προς τους καταναλωτές φορείς (π.χ. τράπεζες, τηλεπικοινωνιακές εταιρείες, κυβερνητικές υπηρεσίες κ.α.) και τα οποία θα μπορούν να χρησιμοποιηθούν μόνο εφόσον δοθεί η σαφής συγκατάθεση του ενδιαφερόμενου πελάτη φαίνεται να έχει τα πλεονεκτήματα της ταχύτερης και ολοκλήρωσης ασφαλών συναλλαγών.

Τα μέλη του δικτύου μπορούν να τοποθετούν πληροφορίες ταυτοποίησης και διάφορες προσωπικές πληροφορίες στο blockchain και να επιλέγουν κατά περίπτωση τη κοινοποίηση τους σε άλλους ενδιαφερόμενους. Με αυτό τον τρόπο μπορούν να παρακαμφθούν «κλειστές» υπηρεσίες ταυτοποίησης όπως είναι αυτές που παρέχονται από τη Google και το Facebook.

8.5 Ασφάλειες

Υπάρχουν πολλά είδη ασφαλειών όπως οι ασφάλειες αυτοκινήτων, οι ασφάλειες ζωής, οι ασφάλειες υγείας κ.α. Οι προκλήσεις που αντιμετωπίζει ο κλάδος των ασφαλειών είναι πολλές με σημαντικότερες από αυτές τις απόπειρες απάτης, την αποδοτική διαχείριση των

[27] http://www.ktimatologio.gr/

συναλλαγών με τρίτα μέλη και τη διαχείριση μεγάλων ποσοτήτων δεδομένων. Το blockchain μπορεί να βοηθήσει έτσι ώστε ο κλάδος των ασφαλειών να λειτουργήσει αποδοτικότερα παρέχοντας εμπιστοσύνη, σταθερότητα και διαφάνεια. Η ύπαρξη ενός δημόσιου κοινού καθολικού μπορεί να αποτρέψει τον πλεονασμό (επανάληψη της πληροφορίας) ενώ οι ταυτότητες των πελατών, οι πολιτικές ασφάλισης και οι συναλλαγές μπορούν να επαληθεύονται μέσω του blockchain. Από την άλλη μεριά η υποκλοπή πληροφοριών καθίσταται δυσκολότερη για τους επίδοξους hackers.

Τα έξυπνα συμβόλαια προσφέρουν την προοπτική αντικατάστασης των συμβολαίων σε χαρτί με πλήρως ηλεκτρονικά συμβόλαια και κατ' επέκταση τη μείωση χρόνου και κόστους. Οι συναλλαγές με τρίτα μέλη καθίστανται ευκολότερα επαληθεύσιμες. Δίνεται η δυνατότητα στις ασφαλιστικές εταιρείες να ανακαλούν διεκδικήσεις ασφαλισμένων που έχουν συμβεί στο παρελθόν και να αντιμετωπίζουν αποτελεσματικότερα περιπτώσεις απάτης. Στο blockchain μπορούν να αποθηκευτούν απευθείας ή μέσω αναφορών τεράστιες ποσότητες δεδομένων στις οποίες μπορούν να έχουν πρόσβαση όλοι οι ενδιαφερόμενοι. [11]

8.6 Υγεία

Οι υπηρεσίες υγείας χρειάζονται έναν αποδοτικότερο και ασφαλέστερο τρόπο διαχείρισης των ιατρικών φακέλων ασθενών καθώς και της διαχείρισης των οικονομικών δεδομένων που δημιουργούνται στην πορεία των ασθενών εντός του συστήματος υγείας. Η τρέχουσα κατάσταση σε ότι αφορά τους ιατρικούς φακέλους ασθενών είναι ότι στην καλύτερη περίπτωση διατηρούνται σε κάποια κεντρική βάση δεδομένων (πιθανά στο cloud) μιας ιατρικής μονάδας. Η δε πρόσβαση στα δεδομένα των ιατρικών φακέλων μπορεί να γίνει μόνο από το προσωπικό της ιατρικής μονάδας στην οποία έχουν δημιουργηθεί τα δεδομένα εξαρχής. Αυτή η κατάσταση πέρα από το ότι συνεπάγεται υψηλότερο από το απαιτούμενο κόστος είναι ευάλωτη σε επιθέσεις με στόχο την ασφάλεια των δεδομένων.

Το blockchain δίνει τη δυνατότητα καταγραφής του πλήρους ιατρικού ιστορικού του κάθε ασθενή, επιτρέποντας τη διάθεση της πληροφορίας σε διάφορα επίπεδα λεπτομέρειας όπως αυτά θα ορίζονται από τον ασθενή, τους ιατρούς, ρυθμιστικές αρχές, ασφαλιστές κλπ. Η ύπαρξη των συγκεκριμένων πληροφοριών θα υποχρεώνει τους ασφαλιστικούς φορείς να προσδιορίζουν και να αποδίδουν ταχύτερα τις απαιτούμενες αποζημιώσεις, ενώ αναλυτικό ιστορικό του ασθενή με δοσολογίες φαρμάκων και πλήρη στοιχεία περίθαλψης θα είναι προσβάσιμα στο εξουσιοδοτημένο ιατρικό προσωπικό έτσι ώστε να αποφασίσει την περαιτέρω αγωγή εάν και όταν παρουσιαστεί η σχετική ανάγκη.

8.7 Φαρμακευτικές

Ένα πρόβλημα που καλούνται να αντιμετωπίσουν οι φαρμακευτικές εταιρείες είναι η κυκλοφορία αντιγράφων φαρμάκων που παράγονται και διατίθενται με μη ελεγχόμενους τρόπους θέτοντας σε κίνδυνο τη δημόσια υγεία. Το blockchain θεωρητικά δίνει τη δυνατότητα να καταγράφεται το πλήρες ιστορικό κάθε συσκευασίας φαρμάκου από την παραγωγή του μέχρι την τελική λιανική του πώληση συμπεριλαμβανομένων όλων των ενδιάμεσων σταθμών από τους οποίους περνά η συσκευασία κατά τη μεταφορά της.

8.8 Εκπαίδευση

Η εκπαίδευση αποτελεί έναν κλάδο που φαίνεται να μπορεί να βελτιωθεί μέσω του blockchain[28]. Πληροφορίες που αφορούν τις σπουδές μαθητών και φοιτητών από την έναρξή μέχρι και την ολοκλήρωσή τους μπορούν να διατηρούνται μόνιμα στο blockchain. Η συγκεκριμένη τεχνολογία φαίνεται να είναι σε θέση να αντιμετωπίσει προβλήματα που έχουν να κάνουν με την ασφαλή διακίνηση προσωπικών δεδομένων και την αντιμετώπιση περιστατικών διαρροής δεδομένων που συχνά βλέπουν το φως της δημοσιότητας[29]. Επιπλέον, η πληροφορία που είναι καταγεγραμμένη στο blockchain μπορεί να δίνει σε εν δυνάμει εργοδότες διασφάλιση ότι οι υποψήφιοι εργαζόμενοι έχουν ολοκληρώσει τις σπουδές που ισχυρίζονται και έχουν λάβει τις επιθυμητές πιστοποιήσεις. Ωστόσο, η ιδιωτικότητα και η παροχή πιστοποιητικών δεν είναι οι μοναδικές εφαρμογές του blockchain στην εκπαίδευση και ορισμένες επιπλέον ενδεικτικές εφαρμογές αναφέρονται στη συνέχεια:

- Προετοιμασία για τις εξετάσεις: Το blockchain μπορεί να χρησιμοποιηθεί για να συνδεθούν σπουδαστές με καθηγητές και βοηθούς καθηγητών έτσι ώστε η μεταφορά γνώσεων να γίνεται προσωποποιημένα και αποδοτικότερα.
- Υπηρεσίες πληροφόρησης: Οι αυξημένες δυνατότητες του blockchain για αποθήκευση και διαμοιρασμό πληροφορίας το καθιστά ως κατάλληλο για την καταγραφή πληροφοριών που διακινούνται εντός μιας εκπαιδευτικής μονάδας όπως για παράδειγμα το πρόγραμμα μαθημάτων και των αλλαγών που πραγματοποιούνται σε αυτό καθώς εξελίσσονται τα επιστημονικά αντικείμενα.

8.9 Κατοχύρωση πνευματικής ιδιοκτησίας

Μουσικοί και άλλοι παραγωγοί πνευματικού περιεχομένου μπορούν, μέσω του blockchain, να βρίσκονται σε άμεση επικοινωνία με το κοινό τους έτσι ώστε να διευκολύνεται η εύρεση, η διάθεση και η δίκαιη αμοιβή των παραγωγών χωρίς να επιβάλλονται χρεώσεις που αποδίδονται σε τρίτους. Εκτιμάται ότι το blockchain αποτελεί λύση στο θέμα της διαφάνειας σε σχέση με την πατρότητα του πνευματικού περιεχομένου, δηλαδή να μπορεί κάποιος να αποδείξει ότι είναι ο πραγματικός δημιουργός ενός διεκδικούμενου και από άλλους περιεχομένου [12]. Επιπλέον, το blockchain μειώνει τον κίνδυνο ηλεκτρονικής πειρατείας επιτρέποντας έλεγχο πάνω στα ψηφιακά αντίγραφα που δημιουργούνται αλλά και μια δευτερεύουσα αγορά ήδη «χρησιμοποιημένου» ψηφιακού περιεχομένου. Επιτρέπει να συνδυαστούν διάφορες άδειες χρήσης περιεχομένου (συμπεριλαμβανομένων των creative commons[30]) με μοντέλα εσόδων για τους δημιουργούς που εξυπηρετούνται μέσω έξυπνων συμβολαίων και πληρωμών σε κρυπτονομίσματα.

Από την άλλη μεριά υπάρχουν πολλά ανοικτά θέματα που θα πρέπει να διευθετηθούν έτσι ώστε το blockchain να μπορεί να εφαρμοστεί στην κατοχύρωση πνευματικής ιδιοκτησίας, στην πράξη. Ενδεικτικά αναφέρεται το θέμα του που θα αποθηκεύονται τα ίδια τα copyrighted περιεχόμενα (στο blockchain ή εκτός blockchain) και το θέμα του ποιο είναι το κατάλληλο σημείο ισορροπίας ανάμεσα στη μη τροποποιήσιμη φύση του blockchain και στην ανάγκη ενημέρωσης της αποθηκευμένης πληροφορίας η οποία σε ορισμένες περιπτώσεις γίνεται με μη άτυπο τρόπο.

[28] https://dataconomy.com/2019/01/how-will-blockchain-transform-the-education-system/
[29] https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017
[30] https://creativecommons.org/licenses/?lang=el

8.10 Ηλεκτρονική ψηφοφορία

Το πρόβλημα της ηλεκτρονικής ψηφοφορίας παρουσιάζει ορισμένα αντικρουόμενα χαρακτηριστικά. Για παράδειγμα θα πρέπει να διασφαλίζεται η ανωνυμία της ψήφου αλλά ταυτόχρονα θα πρέπει να υπάρχει κάποιος τρόπος επαλήθευσης των αποτελεσμάτων έτσι ώστε να αποφεύγεται η παραποίηση των αποτελεσμάτων. Από την άλλη μεριά ο τρόπος με τον οποίο διεξάγονται οι ψηφοφορίες σήμερα φαίνεται να βρίσκεται σε αναντιστοιχία με την ψηφιακή εποχή την οποία βιώνουμε. Η χρήση συστημάτων ηλεκτρονικής ψηφοφορίας επιτρέπει τη συμμετοχή στη ψηφοφορία χωρίς να απαιτείται η φυσική παρουσία, την άμεση έκδοση αποτελεσμάτων, την αποφυγή επανάληψης καταμέτρησης κ.α. Η τεχνολογία blockchain φαίνεται να προσθέτει ορισμένα επιπλέον επιθυμητά χαρακτηριστικά όπως για παράδειγμα την αδυναμία αλλαγής της ψήφου από τι στιγμή που εισάγεται στο blockchain και μετά. Ένα παράδειγμα συστήματος ηλεκτρονικής ψηφοφορίας το οποίο χρησιμοποιεί τη τεχνολογία blockchain είναι το Follow My Vote[31]. Ωστόσο, υπάρχει προβληματισμός του κατά πόσο μπορεί να εφαρμοστεί στην πράξη καθώς η κατανεμημένη φύση του, η τεχνολογική του πολυπλοκότητα και η τρέχουσα νομοθεσία δεν το ευνοούν έτσι ώστε να υιοθετηθεί μαζικά.

[31] https://followmyvote.com/

9 Ιδιωτικά blockchains

Τα ιδιωτικά blockchains είναι blockchains που απευθύνονται σε μια επιχείρηση ή σε μια ομάδα επιχειρήσεων με την ταυτότητα όλων των χρηστών του συστήματος να είναι γνωστή. Σε ένα ιδιωτικό blockchain δίνεται η δυνατότητα περιορισμού στο ποιος μπορεί να συνδεθεί σε αυτό. Πρόκειται στην ουσία για κατανεμημένες βάσεις δεδομένων που επιτρέπουν στα μέλη τους να αποφασίσουν για το ποιος μπορεί να συμμετάσχει στο μηχανισμό συναίνεσης και ποιοι μπορούν να επαληθεύουν τις συναλλαγές. Οι δε κόμβοι ενός ιδιωτικού blockchain αποκτούν τη δυνατότητα να εγγράφουν πληροφορίες στο blockchain μέσω των εγγεγραμμένων και επαληθευμένων μελών.

Σημαντικές περιπτώσεις ιδιωτικών blockchains είναι:

- Corda
- Hyperledger
- Multichain
- Quorum
- Sequence

9.1 Σύγκριση ιδιωτικών blockchains με δημόσια blockchains

Η σύγκριση ιδιωτικών με δημόσια blockchains δεν βγάζει κάποιον καθαρό νικητή[32]. Αν και η βάση της τεχνολογίας τους είναι η ίδια (το blockchain), φαίνεται να εστιάζουν σε διαφορετικές εφαρμογές. Ως βασικά πλεονεκτήματα των ιδιωτικών blockchains μπορούν να αναφερθούν τα ακόλουθα:

- **Υψηλότερη απόδοση**: Λόγω του ότι στα ιδιωτικά blockchain η επαλήθευση των συναλλαγών γίνεται από γνωστά και αξιόπιστα μέλη οι μηχανισμοί συναίνεσης που χρησιμοποιούνται είναι πολύ περισσότερο αποδοτικοί από τους μηχανισμούς που χρησιμοποιούν τα δημόσια blockchains. Για παράδειγμα αντί του ενεργοβόρου μηχανισμού PoW (Proof of Work) που χρησιμοποιεί το bitcoin, στα ιδιωτικά blockchains χρησιμοποιείται ο μηχανισμός PoS (Proof of Stake) ή κάποια παραλλαγή του που λειτουργεί ως ψηφοφορία στην οποία συμμετέχουν μόνο επιλεγμένα μέλη του δικτύου. Το αποτέλεσμα είναι να υπάρχει μικρότερη απαίτηση για υπολογιστική ισχύ και υψηλότερος ρυθμός συναλλαγών που μπορεί να υποστηριχθεί.
- **Ευκολότερη προσαρμογή σε νέες καταστάσεις**: Οι αποφάσεις για το πως θα προσαρμοστεί ένα ιδιωτικό blockchain σε νέες καταστάσεις λαμβάνονται ταχύτερα και συμμετέχουν σε αυτές μόνο οι άμεσα ενδιαφερόμενες επιχειρήσεις. Το λογισμικό ενημερώνεται συχνότερα.

Ωστόσο, μπορούν να εντοπιστούν και μειονεκτήματα των ιδιωτικών blockchains όπως τα ακόλουθα:

- **Ασφάλεια**: Η ασφάλεια ενός ιδιωτικού blockchain εξαρτάται εξ' ολοκλήρου από την ακεραιότητα των μελών του.
- **Εξάρτηση από συγκεκριμένα μέλη του δικτύου**: Υπάρχει ο κίνδυνος συνασπισμού ισχυρών μελών του ιδιωτικού blockchain έτσι ώστε να επιβάλλουν το τι θα είναι σε θέση να καταγραφεί σε αυτό.

[32] https://monax.io/learn/permissioned_blockchains/

9.2 Hyperledger

Το Hyperledger[33] έχει αναπτυχθεί υπό την αιγίδα του Linux Foundation και συμμετέχουν σε αυτό πάνω από 270 γνωστές εταιρείες και οργανισμοί από το χώρο της τεχνολογίας (π.χ. Cisco, IBM, Intel) από το χρηματοοικονομικό κλάδο (π.χ. ABN AMRO, J.P. Morgan), από το χώρο των επιχειρήσεων (π.χ. SAP), εκπαιδευτικοί οργανισμοί (π.χ. UCLA Blockchain lab). Είναι ένα λογισμικό ανοικτού κώδικα μέσω του οποίου μπορούν να χτιστούν εφαρμογές έξυπνων συμβολαίων χωρίς να χρησιμοποιούνται δημόσια blockchains όπως τα blockchains του Bitcoin και του Ethereum. Η βασική ιδέα είναι ότι αντί κάθε επιμέρους βιομηχανία να δημιουργεί τη δική της blockchain λύση, να χρησιμοποιηθεί μια κοινά αποδεκτή πλατφόρμα αποτελούμενη από επιμέρους τμήματα τα οποία μπορούν να επιλεχθούν και να συνδυαστούν έτσι ώστε να παρέχουν λύσεις σε κάθετα πεδία εφαρμογών. Ιδιαίτερη δε έμφαση έχει δοθεί στην υποστήριξη εφαρμογών που αφορούν την εφοδιαστική αλυσίδα (supply chain).

Στο Hyperledger η πληροφορία που καταγράφεται στο blockchain δεν είναι δημόσια διαθέσιμη. Ορίζεται όμως η έννοια των καναλιών σύμφωνα με την οποία μόνο τα εμπλεκόμενα μέλη μιας συναλλαγής έχουν πρόσβαση στα δεδομένα της συναλλαγής καθώς μόνο αυτά μπορούν να «ακούνε» τα δεδομένα της συναλλαγής.

Τα μέλη ενός blockchain συστήματος που στηρίζεται στο Hyperledger αποφασίζονται από οντότητες στις οποίες ανατίθεται η συγκεκριμένη αρμοδιότητα. Σε κάθε μέλος ανατίθεται ένας ρόλος που καθορίζει τα δικαιώματα προσπέλασης και επαλήθευσης δεδομένων που διαθέτει. Ειδικότερα υπάρχουν τρεις ρόλοι: οι orderers που υποβάλουν τις συναλλαγές, οι endorsers που επαληθεύουν τις συναλλαγές και οι commiters που πρέπει να καταλήξουν σε συμφωνία προκειμένου να καταγραφούν οι συναλλαγές στο blockchain.

Γενικά τα έργα τα οποία στηρίζονται στο Hyperledger έχουν μια αρθρωτή δομή και ανάλογα με την εφαρμογή επιλέγονται και εξειδικεύονται επιμέρους τμήματά του όπως αυτά που φαίνονται στην Εικόνα 18.

Εικόνα 18. Τμήματα (modules) του HYPERLEDGER

Στη συνέχεια παρουσιάζονται με συντομία μερικά από τα σημαντικότερα επιμέρους τμήματα του HyperLedger.

[33] https://www.hyperledger.org/

9.2.1 Hyperledger Fabric

Το Hyperledger Fabric είναι ένα ιδιωτικό blockchain στο οποίο τα μέλη συνδέονται μέσω ενός MSP (Membership Service Provider). Πολλά από τα χαρακτηριστικά του Fabric μπορούν να προσαρμοστούν ενώ δίνεται η δυνατότητα επιλογής των δυνατοτήτων που είναι επιθυμητό να παρέχονται. Τα δεδομένα του καθολικού μπορούν να αποθηκεύονται με διάφορες εσωτερικές διαμορφώσεις, μπορεί να επιλέγεται ο μηχανισμός συναίνεσης ενώ υπάρχουν και διάφοροι τύποι MSP που υποστηρίζονται.

Το Fabric παρέχει τη δυνατότητα της δημιουργίας καναλιών, που επιτρέπουν σε μια ομάδα συμμετεχόντων να δημιουργήσουν ένα ξεχωριστό καθολικό συναλλαγών. Αν για παράδειγμα δύο συμμετέχοντες δημιουργήσουν ένα κανάλι, τότε μόνο αυτοί έχουν αντίγραφα του καθολικού του συγκεκριμένου καναλιού.

Το υποσύστημα που διαθέτει το Fabric για το καθολικό αποτελείται από δύο τμήματα: το world state (βάση δεδομένων) και το transaction log (blockchain). Το τμήμα world state αφορά την κατάσταση του καθολικού στην τρέχουσα χρονική στιγμή ενώ το transaction log περιέχει όλες τις συναλλαγές που οδήγησαν σε αυτή τη κατάσταση.

Ο κώδικας των έξυπνων συμβολαίων γράφεται σε chaincode και μπορεί να υλοποιηθεί χρησιμοποιώντας διάφορες γλώσσες προγραμματισμού. Με τη χρήση του chaincode μπορούν να οριστούν πόροι (assets) και οι οδηγίες συναλλαγών που τροποποιούν ιδιότητές τους.

9.2.2 Hyperledger Burrow

Το Hyperledger Burrow είναι ένα ιδιωτικό blockchain που λειτουργεί ανάλογα με το blockchain του Ethereum. Η βασική λειτουργία του είναι η εκτέλεση έξυπνων συμβολαίων με αποδοτικό τρόπο. Το Burrow επιδιώκει να είναι ένα γρήγορο και ελαφρύ ιδιωτικό καθολικό και να αποτελέσει ένα EVM, που θα είναι σε θέση να ενσωματωθεί με σχετική ευκολία σε διάφορες εφαρμογές.

9.2.3 Hyperledger Composer

Το Hyperledger Composer ορίζει ένα προγραμματιστικό μοντέλο που επιτρέπει να οριστούν και να εγκατασταθούν επιχειρηματικά δίκτυα και εφαρμογές μέσω των οποίων συμμετέχοντες είναι σε θέση να πραγματοποιούν συναλλαγές προκειμένου να επιτευχθεί διακίνηση πόρων.

Το Hyperledger Composer έχει κατασκευαστεί με τέτοιο τρόπο έτσι ώστε να επιτρέπει τη συνεργασία επιχειρηματιών και προγραμματιστών απευθείας έτσι ώστε από κοινού να ορίσουν την επιχειρηματική διαδικασία που είναι επιθυμητό να αποτυπωθεί. Παρέχεται μάλιστα η διαδικτυακή υπηρεσία Hyperledger Composer Playground που μπορεί να χρησιμοποιηθεί για αρχική σχεδίαση και έλεγχο ιδεών.

9.2.4 Hyperledger Explorer

Το Hyperledger Explorer είναι μια βοηθητική εφαρμογή που επιτρέπει τη δημιουργία διαδικτυακών διεπαφών μέσω των οποίων ο χρήστης μπορεί να εντοπίσει χρήσιμες πληροφορίες για το blockchain δίκτυο. Μέσω γραφημάτων παρουσιάζεται μια κατανοητή εικόνα κρίσιμων μεγεθών του δικτύου. Εμφανίζει πληροφορίες που αφορούν τους κόμβους του δικτύου, λεπτομέρειες για τα μπλοκ του blockchain, στοιχεία συναλλαγών και γενικότερα οποιαδήποτε πληροφορία αφορά το blockchain δίκτυο.

10 Προβληματισμοί σχετικά με το blockchain

Η τεχνολογία blockchain έχει δημιουργήσει υψηλές προσδοκίες και πολλές φορές παρουσιάζεται ως πανάκεια. Ωστόσο, υπάρχει προβληματισμός σχετικά με το εάν θα καταφέρει να επιφέρει τις αλλαγές που οι υποστηρικτές της ισχυρίζονται. Ορισμένα προβλήματα που πρέπει να ξεπεραστούν έχουν να κάνουν με το ρυθμό συναλλαγών που μπορεί να υποστηρίξει, με το ενεργειακό κόστος που συνεπάγεται[34], με την ασφάλεια που προσφέρει[35] και με την πιθανή συσχέτισή της συγκεκριμένης τεχνολογίας με εγκληματικές ενέργειες σε ορισμένες εφαρμογές όπως τα κρυπτονομίσματα[36]. Η ανωριμότητα της τεχνολογίας blockchain έχει φανεί σε περιπτώσεις που βλέπουν το φως της δημοσιότητας όπως για παράδειγμα το hard fork του Ethereum[37] και η αλλαγή του μεγέθους μπλοκ του bitcoin[38].

Σημαντικότερο πρόβλημα ωστόσο αποτελεί η προσπάθεια προσαρμογής οποιασδήποτε επιχειρηματικής ιδέας έτσι ώστε να περιλαμβάνει το blockchain. Λόγω των υπερπροσδοκιών που έχουν δημιουργηθεί προτείνονται έργα που χρησιμοποιούν blockchain ενώ η χρήση ενός συστήματος διαχείρισης βάσεων δεδομένων όπως η Oracle, ο Microsoft SQL Server ή ακόμα και τα ανοικτού κώδικα λογισμικά βάσεων δεδομένων MySQL και Postgress επαρκούν. Το συμπέρασμα είναι ότι το blockchain αποτελεί μια «κακή» λύση αν οι προδιαγραφές καλύπτονται επαρκώς από ένα σχεσιακό σύστημα βάσεων δεδομένων. Ο λόγος είναι ότι τα συστήματα σχεσιακών βάσεων δεδομένων έχουν αναπτυχθεί για δεκαετίες, έχουν εγκατασταθεί, λειτουργούν με επιτυχία σε εκατομμύρια εξυπηρετητές σε όλο τον κόσμο και εξυπηρετούν ακόμα περισσότερους χρήστες με αποδοτικό τρόπο. Τεχνολογίες όπως η κλωνοποίηση Βάσεων Δεδομένων (replicated databases) και οι πλέον πρόσφατες NoSQL Βάσεις Δεδομένων καλύπτουν ακόμα μεγαλύτερο ευρύτερο πεδίο εφαρμογών χωρίς να χρειάζεται κανείς να χρησιμοποιήσει blockchain.

Σύμφωνα με την ηλεκτρονική δημοσίευση [13] για να προσθέτει αξία το blockchain σε ένα έργο θα πρέπει να ικανοποιούνται όλοι οι ακόλουθοι περιορισμοί:

- **Ανάγκη ύπαρξης Βάσης Δεδομένων**. Πρέπει να υπάρχει ανάγκη καταγραφής πληροφορίας που πρόκειται να διαμοιραστεί σε πολλούς χρήστες. Στην περίπτωση του blockchain η Βάση Δεδομένων αναφέρεται ως καθολικό (ledger).
- **Ύπαρξη πολλών χρηστών που επιθυμούν να γράφουν στη Βάση Δεδομένων**. Εκτός από τους χρήστες που διαβάζουν μόνο δεδομένα από τη Βάση Δεδομένων θα πρέπει κάποιοι από αυτούς και να γράφουν δεδομένα. Οι χρήστες αυτοί στην περίπτωση του blockchain αποτελούν κόμβους του συστήματος και διατηρούν αντίγραφό του καθολικού και ενημερώνουν για τις αλλαγές που πραγματοποιούν τους ομότιμους κόμβους του συστήματος.
- **Απουσία εμπιστοσύνης**. Θα πρέπει να υπάρχει κάποιος βαθμός απουσίας εμπιστοσύνης ανάμεσα στις οντότητες που χρησιμοποιούν το σύστημα. Σε ένα σύστημα blockchain δεν υπάρχει η έννοια της «αυθαίρετης» τροποποίησης των δεδομένων, όπως μπορεί να συμβεί σε μια παραδοσιακή Βάση Δεδομένων. Οι

[34] https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency
[35] https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/
[36] https://blockonomi.com/history-of-silk-road/
[37] https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds
[38] https://techcrunch.com/2015/08/22/money-and-politics-bitcoins-governance-crisis/

υπόλοιποι χρήστες δεν είναι υποχρεωμένοι να δέχονται ως την «απόλυτη αλήθεια» την καταγραφή δεδομένων από οποιονδήποτε από τους χρήστες με δικαίωμα εγγραφής.

- **Αποδιαμεσολάβηση**. Θα πρέπει να απουσιάζει κάποιος έμπιστος διαμεσολαβητής. Το blockchain επιτρέπει σε πολλούς χρήστες με δικαίωμα εγγραφής που δεν εμπιστεύονται ο ένας τον άλλον να τροποποιούν απευθείας το καθολικό. Η υπόθεση αυτή είναι πολύ ισχυρή. Θα πρέπει να σημειωθεί ότι αν σε ένα σύστημα υπάρχει κάποια οντότητα που μπορεί να λειτουργήσει ως έμπιστος διαμεσολαβητής για όλους τους άλλους τότε τα πλεονεκτήματα χρήσης του blockchain παύουν να υφίστανται σε μεγάλο βαθμό.
- **Αλληλεπίδραση συναλλαγών**. Για να έχει νόημα η χρήση του blockchain θα πρέπει οι συναλλαγές που καταγράφονται από έναν χρήστη να εμπεριέχουν κοινά στοιχεία με άλλες συναλλαγές και σε κάποιο βαθμό να αλληλεξαρτώνται. Μια καλή περίπτωση χρήσης αποτελεί η περίπτωση στην οποία υφίστανται αλληλοσχετιζόμενες συναλλαγές χρηστών ακόμα και αν τα ίδια τα δεδομένα παραμένουν ανεξάρτητα. Αυτό συμβαίνει για παράδειγμα σε μια Βάση Δεδομένων ταυτοτήτων όπου διάφορες οντότητες επαληθεύουν διάφορα στοιχεία που σχετίζονται με τις ταυτότητες των συμμετεχόντων. Αν και κάθε μια από τις οντότητες είναι ανεξάρτητη, το blockchain προσφέρει την απαιτούμενη ενοποιημένη εικόνα.
- **Καθορισμός κανόνων**. Θα πρέπει να υπάρχουν σαφώς ορισμένοι κανόνες που να ορίζουν πότε οι συναλλαγές είναι έγκυρες. Για παράδειγμα σε καθολικά που σχετίζονται με καταγραφή πόρων θα πρέπει να διασφαλίζεται ότι δεν δημιουργούνται νέοι πόροι από το μηδέν.
- **Επιλογή επαληθευτών**. Θα πρέπει να αποφασιστεί με σαφήνεια το ποιοι θα είναι οι επαληθευτές και με ποιο τρόπο διασφαλίζεται ότι συνολικά το σύστημα είναι έμπιστο. Αυτό μπορεί να σημαίνει ότι οι επαληθευτές ελέγχονται από έναν οργανισμό ή από ένα σύνολο οργανισμών ή ακόμα και από το σύνολο των ίδιων των επαληθευτών μέσω ενός μηχανισμού PoW.
- **Υποστήριξη των φυσικών πόρων που καταγράφονται στη Βάση Δεδομένων**. Αν το blockchain πρόκειται να χρησιμοποιηθεί για την καταγραφή πόρων με φυσική υπόσταση, θα πρέπει να υπάρχει κάποιος υπεύθυνος οργανισμός που θα αναλάβει την πλήρη αντιστοίχιση για οτιδήποτε καταγράφεται στο blockchain στον φυσικό κόσμο με ότι σημαίνει αυτό για τις υποχρεώσεις αποζημίωσης.

Στο ίδιο πνεύμα οι συγγραφείς του άρθρου [14] εκφράζουν τον προβληματισμό τους για τις ουσιαστικές χρήσεις του blockchain. Παραθέτουν μάλιστα την Εικόνα 19 που αναπαριστά ένα διάγραμμα ροής για τη λήψη απόφασης σχετικά με το εάν απαιτείται να χρησιμοποιηθεί σε ένα έργο η τεχνολογία blockchain. Οι απαντήσεις που εξάγονται από το διάγραμμα ροής είναι μία από τις ακόλουθες περιπτώσεις:

- μη χρήση blockchain (συχνότερα)
- χρήση ιδιωτικού blockchain με ελεγχόμενες συμμετοχές
- χρήση δημόσιου blockchain με ελεγχόμενες συμμετοχές
- χρήση blockchain με ελεύθερες συμμετοχές (σπανιότερα)

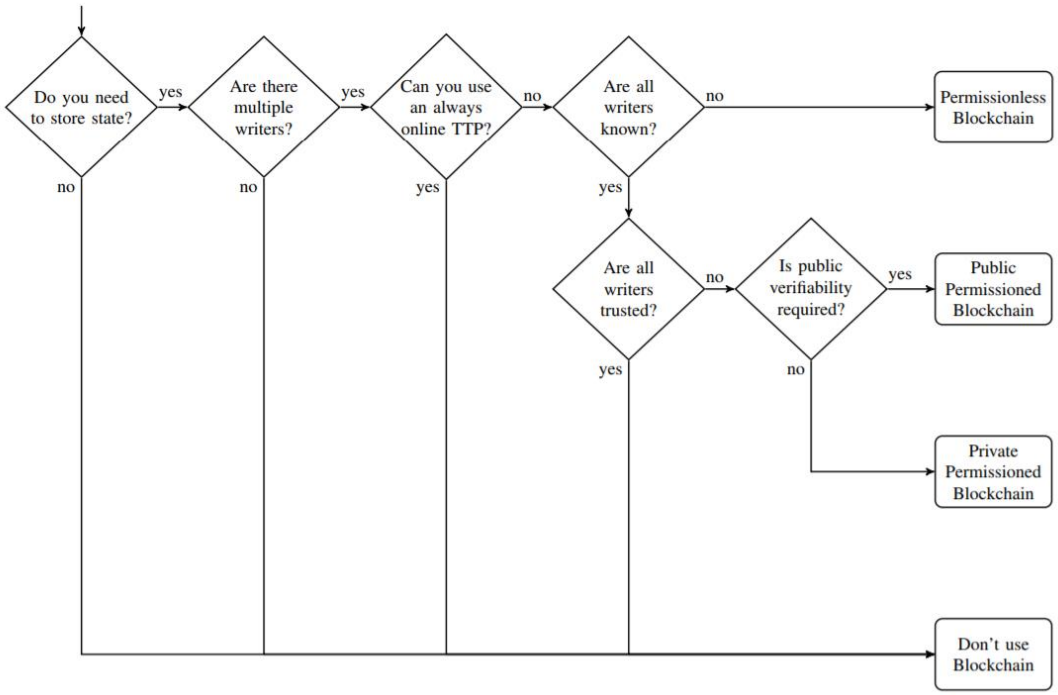


Fig. 1: A flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem (Table I should be considered in the decision making process as well). Writers refer to entities with write access to the database/blockchain, i.e. in a blockchain setting, a writer corresponds to a consensus participant. If a trusted third party (TTP) is available that is not always online, this can be used to establish a known group of writers, i.e. the TTP can function as a certificate authority in such a setting. Public and private permissioned blockchains differ in that a public blockchain allows anyone to read the contents of the chain and thus verify the validity of the stored data, while a private blockchain only allows a limited number of participants to read the chain. Note that for any blockchain based solution it is possible to make use of cryptographic primitives in order to hide privacy-relevant content.

Εικόνα 19. Do you need a blockchain? [14]

Τέλος, αξίζει να αναφερθεί η ηλεκτρονική δημοσίευση [15] που εντοπίζει 3 περιπτώσεις στις οποίες εκτιμά ότι η χρήση του blockchain δεν αποτελεί λύση για τις επιχειρήσεις σήμερα. Οι περιπτώσεις αυτές είναι οι ακόλουθες:

1. Περίπτωση στην οποία μια επιχείρηση πρόκειται να χρησιμοποιήσει το blockchain για εργασία που θα πραγματοποιηθεί χωρίς την εμπλοκή εξωτερικών εταίρων.
2. Περίπτωση που απαιτεί χειρισμό πολλών ειδικών καταστάσεων όπως και εξαιρέσεων σε αυτές.
3. Περίπτωση που απαιτεί πολύ υψηλή απόδοση (π.χ. εκατομμύρια συναλλαγές ανά δευτερόλεπτο).

11 Επίλογος – συμπεράσματα

Στο Δεκέμβριο του 2017, σχεδόν 8 έτη μετά από την εμφάνισή του bitcoin, η αξία 1 BTC όπως καταγράφεται στο https://www.xe.com/ έφτασε στην υψηλότερη μέχρι σήμερα (Μάϊος 2019) τιμή της, στα 16.548,13€[39]. Λίγο μετά από το bitcoin παρουσιάστηκαν εκατοντάδες άλλα κρυπτονομίσματα (LTC, XMR, XRP κ.α.) και αρκετά από αυτά διαγράφουν επιτυχημένη πορεία μέχρι και σήμερα. Το 2017 και το 2018 αποτέλεσαν έτη στα οποία η τεχνολογία blockchain, στην οποία στηρίζεται το bitcoin και τα άλλα κρυπτονομίσματα, ήταν συνεχώς στη δημοσιότητα και το ίδιο φαίνεται να συμβαίνει και στο 2019. Η τεχνολογία blockchain έχει χαιρετιστεί ως πρωτοποριακή και πολλοί πιστεύουν ότι πρόκειται να επιφέρει αλλαγές στην κοινωνία γενικότερα ανάλογες με αυτές που έφερε το διαδίκτυο. Ωστόσο, υπάρχει και από μια άλλη μερίδα ατόμων σκεπτικισμός σχετικά με το εάν πρόκειται για κάποια «μόδα» και κατά πόσο αναμένεται σύντομα να υπάρξουν επιτυχημένες εφαρμογές που να στηρίζονται στο blockchain και οι οποίες θα πετύχουν ανατάραξη σε επιχειρηματικούς κλάδους όπως οι τράπεζες, οι ασφάλειες κ.α.

Στην παρούσα πτυχιακή εργασία εξετάστηκαν βασικές ιδέες που σχετίζονται με τη λειτουργία το blockchain όπως είναι ο κατακερματισμός, οι κρυπτογραφικές συναρτήσεις κατακερματισμού, η κρυπτογραφία, οι μηχανισμοί εξασφάλισης συναίνεσης, τα δένδρα Merkle, το πρόβλημα της συμφωνίας των Βυζαντινών στρατηγών και το πρόβλημα απόδειξης μηδενικής γνώσης. Εξετάστηκε η έννοια των έξυπνων συμβολαίων και παρουσιάστηκαν πιθανά πεδία εφαρμογών τους στους χώρους των ασφαλειών, της αγοραπωλησίας ακινήτων, της ηλεκτρονικής διακυβέρνησης, των πνευματικών δικαιωμάτων, της παροχής πιστοποιητικών και αλλού.

Παρουσιάστηκε η διαφορά ανάμεσα στα δημόσια blockchains τύπου Bitcoin και Ethereum και στα ιδιωτικά blockchains (π.χ. Hyperledger) για τα οποία φαίνεται να υπάρχει μεγάλο ενδιαφέρον από μεγάλες εταιρείες τεχνολογίας αλλά και χρηματοοικονομικούς οργανισμούς. Εξετάστηκε κριτικά η προοπτική της τεχνολογίας blockchain και παρουσιάστηκαν πλεονεκτήματα αλλά και μειονεκτήματα που εντοπίστηκαν.

Είναι πιθανόν στην επόμενη δεκαετία η τεχνολογία blockchain να έχει ενσωματωθεί στην καθημερινότητά μας και να θεωρούμε αυτονόητο, για παράδειγμα, ότι θα υπάρχει υπηρεσία που θα είναι σε θέση να παρέχει πληροφορίες για την ταυτότητά του καθενός μας όταν αυτό απαιτείται και χωρίς χρονοβόρες διαδικασίες. Επιπλέον, η διατήρηση αυτής της πληροφορίας ενδέχεται να μην είναι ευθύνη μόνο του κράτους άλλα να εμπλέκονται και διάφορες άλλες οντότητες (π.χ. μη κερδοσκοπικοί οργανισμοί), υπεύθυνες για την επαλήθευση οποιασδήποτε τροποποίησης στα δεδομένα. Με αυτό τον τρόπο, δηλαδή με πολλούς «ελεγκτές» της ορθής λειτουργίας του συστήματος, θα ενισχύεται η ασφάλεια, θα διασφαλίζεται η ιδιωτικότητα και θα αποτρέπονται περιστατικά απάτης. Για να συμβεί αυτό θα πρέπει η τεχνολογία blockchain να ωριμάσει, να διευθετηθούν ανοικτά θέματα που έχουν να κάνουν με τη νομοθεσία, να υπάρξει αποδοχή από τις κυβερνήσεις των κρατών και βέβαια να προσφέρει ουσιαστικά πλεονεκτήματα στην καθημερινότητα των χρηστών του.

[39] Στις 4-Μαϊου-2019 η τιμή του bitcoin ήταν 5.163,33€

Αναφορές

[1] M. E. Peck, «Blockchains: How They Work and Why They'll Change the World,» 2017.

[2] «Τι είναι ή τεχνολογία Blockchain,» [Ηλεκτρονικό]. Available: http://blockchain.org.gr/home/mathe/.

[3] «Top 14 Blockchain Companies to Watch in 2018,» [Ηλεκτρονικό]. Available: https://www.entrepreneur.com/article/308558.

[4] M. Gupta, Blockchain for dummies, 2nd IBM Limited Edition, John Wiley & Sons, Inc., 2018.

[5] L. Lamport, R. Shostak και M. Pease, «The Byzantine general problem,» *ACM Transactions on Programming languages and Systems,* pp. 382-401, 1982.

[6] S. Goldwasser, S. Micali και C. Rackoff, «The knowledge complexity of interactive proof systems,» *SIAM, Journal on Computing,* pp. 186-208, 1989.

[7] N. Satoshi, «Bitcoin: a peer-to-peer electronic cash system,» 2008.

[8] L. W. Cong και H. Zhiguo, «Blockchain Disruption and Smart Contracts».*National Bureau of Economic Research.*

[9] K. Lauslahti, M. Juri και T. Seppälä, «Smart Contracts – How will Blockchain Technology Affect Contractual Practices?,» ETLA Reports, 2017.

[10] M. E. Peck, «How Smart Contracts Work - Blockchain technology could run a flight-insurance business without any employees,» 2017.

[11] «How Blockchain Technology Renovates The Insurance Sectors ?,» [Ηλεκτρονικό]. Available: https://www.bitdeal.net/blockchain-in-insurance.

[12] A. Savelyev, «Copyright in the blockchain era: Promises and challenges,» *Computer Law & Security Review,* pp. 550-561, 6 2018.

[13] G. Greenspan, «Avoiding the pointless blockchain project. How to determine if you've found a real blockchain use case.,» 22 11 2015. [Ηλεκτρονικό]. Available: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.

[14] A. Gervais και K. Wüst, «Do you need a Blockchain?,» σε *Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE*, 2018.

[15] M. v. Rijmenam, «3 Reasons Why You Should Not Use Blockchain in Your Organisation,» 12 12 2018. [Ηλεκτρονικό]. Available: https://vanrijmenam.nl/3-reasons-not-use-blockchain-in-organisation.

[16] D. Drescher, BLOCKCHAIN BASICS - A NON-TECHNICAL INTRODUCTION IN 25 STEPS, Frankfurt am Main, Germany: Apress, 2017.