Πανεπιστήμιο Πατρών

Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Πτυχιακή Εργασία

Τεχνολογία Blockchain και Εφαρμογές

Ονοματεπώνυμο Φοιτητή: Πατσιλίβας Ανδρέας

Εποπτεύον Καθηγητής: Γιωτόπουλος Κωνσταντίνος

Πάτρα, Δεκέμβριος 2020

Περίληψη

Τα τελευταία χρόνια, η τεχνολογία έχει εισβάλει κυριολεκτικά στη ζωή μας. Μαζί της και το Blockchain, το οποίο ως ολοκληρωμένη έννοια παρουσιάστηκε μαζί με το πρώτο κρυπτονόμισμα, το Bitcoin, ως ένας τρόπος διατήρησης δεδομένων, εξασφαλίζοντας πάντα την μοναδικότητα και την εγκυρότητα αυτών, χωρίς την ανάγκη εμπλοκής κάποιας κεντρικής αρχής ελέγχου. Η τεχνολογία είναι σχετικά νέα, αναπτύχθηκε την τελευταία δεκαετία και εκτός από τον χώρο των κρυπτονομισμάτων, από τον οποίο απέκτησε και φήμη, έχει χρήσεις σε μια πληθώρα κλάδων όπως ο νομικός, ο ασφαλιστικός, η εφοδιαστική αλυσίδα, η διαχείριση πνευματικών δικαιωμάτων κ.α. Στην παρούσα εργασία αναλύεται η τεχνολογία του Blockchain καθώς και οι εφαρμογές της στο επιχειρηματικό περιβάλλον. Παρουσιάζονται τεχνικοί όροι όπως χαρακτηριστικά, εκδόσεις, κρυπτογραφία και αλγόριθμοι κατακερματισμού, διευθυνσιοδότηση, ψηφιακή υπογραφή, δημόσια και ιδιωτικά κλειδιά, χαρακτηριστικά των block κ.α. Στη συνέχεια γίνεται αναφορά στους τύπους πρωτοκόλλων συναίνεσης και παρουσιάζονται διάφορα παραδείγματα χρήσης τους. Επιπλέον αναλύεται και ο ρόλος που έχει το κάθε ένα για την επιλογή πλατφόρμας ανάπτυξη εφαρμογής Blockchain. Αναλύονται μερικές από τις πιο δημοφιλείς πλατφόρμες ανάπτυξης εφαρμογών και παραθέτονται παραδείγματα εφαρμογών που έχει το Blockchain στο σημερινό επιχειρηματικό κόσμο. Διάφορα αρνητικά και προβληματισμοί με την χρήση της τεχνολογίας παρουσιάζονται, ενώ παράλληλα προτείνονται και λύσεις για τα διάφορα προβλήματα και ερώτημα που προκύπτουν από τη χρήση. Τέλος γίνεται μία σύνοψη της εργασίας, καταλήγουμε σε συμπεράσματα και σκέψεις για το τι αναμένεται να δούμε στο μέλλον από την τεχνολογία αυτή.

Λέξεις – Κλειδιά

Blockchain, Block, Peer-to-peer, Εξόρυξη, Miner, Αποκέντρωση, Κρυπτονομίσματα, Ψηφιακή Ταυτότητα, Κρυπτογραφία, Αλγόριθμοι Συναίνεσης, Πλατφόρμες Ανάπτυξης Εφαρμογών, Κυβερνοεπιθέσεις.

Abstract

In recent years, technology has literally invaded our lives. Along with it, Blockchain, which as a complete concept was presented back in 2008, together with the first cryptocurrencies as a way of storing data, always ensuring data uniqueness and validity without the need of any central control authority. The technology is relatively new, it is constantly under development and in addition to the field of crypto-currencies from which it gained fame, it has uses in a variety of fields such as law, insurance, supply chain, copyright management, etc. This dissertation aims at a detailed overview of the Blockchain technology as well as its applications in the modern business environment. Technical terms such as features, versions, encryption and fragmentation, address derivation, cryptographic algorithms, digital signature, block characteristics and public-private key ideas are presented. Moreover, the consensus protocols, which are a critical characteristic of a Blockchain network, are also discussed, with an extensive overview of the most widely used ones. In addition, examples of these consensus algorithms are presented with real-world examples. Some of the most popular frameworks, a basic structure underlying a Blockchain system, are overviewed as well. This dissertation also analyzes various negatives and concerns that came with the usage of this technology. However, the thesis also presents solutions for the various problems and questions that arise from the use. Finally, we conclude and we give our thoughts about what is coming and what to expect in the next decades about the Blockchain technology.

Keywords

Blockchain, Block, Peer-to-peer, Mining, Miner, Decentralization, Cryptocurrency, Digital Identity, Cryptography, Consensus Algorithms, Frameworks, Cyber-attacks

Περιεχόμενα

1. Εισαγωγή 1

1.1 Αντικείμενο πτυχιακής εργασίας 1

1.2 Στόχοι της εργασίας 2

1.3 Δομή της εργασίας 2

2. Ανάλυση Τεχνολογικού Περιβάλλοντος 3

2.1 Τεχνολογία Blockchain και αρχιτεκτονική 3

2.1.1 Τύπος Δικτύου 3

2.1.2 Βασικά χαρακτηριστικά του Blockchain 4

2.1.3 Αποκεντρωμένο καθολικό αρχείο 4

2.1.4 Επιπλέον τύποι Blockchain 5

2.1.5 Εκδόσεις του Blockchain 6

2.1.6 Κρυπτογραφημένες συναρτήσεις κατακερματισμού 7

2.1.7 Σετ κλειδιών, ψηφιακή υπογραφή και κρυπτογράφησή της 9

2.1.8 Κρυπτογράφηση Δημόσιου Κλειδιού (PKC) 9

2.1.11 Διευθυνσιοδοτήσεις στα δίκτυα Blockchain 12

2.1.12 Block και τεχνολογικά χαρακτηριστικά 13

2.1.14 Αλυσίδα 15

2.1.15 Τροποποίηση της αλυσίδας (Forking) 16

2.2 Λόγοι χρήσης και μη των Blockchain 17

2.3 Πρωτόκολλα συναίνεσης 18

2.3.1 Proof-of-Work (PoW) 19

2.3.2 Proof-of-Stake (PoS) 19

2.3.3 Υβριδικοί αλγόριθμοι συναίνεσης 21

2.3.4 Proof-of-Elapsed-Time (PoET) 22

2.3.5 Proof-of-Burn (PoB) 22

2.3.6 Proof-of-Authority (PoA) ή Proof-of-Identity (PoI) 23

2.3.7 Delegated-Proof-of-Stake (DPOS) 24

2.3.8 Proof-of-Capacity (PoC) 24

2.3.9 Σύγκριση των αλγορίθμων συναίνεσης 25

2.4 Έξυπνα Συμβόλαια – Smart Contracts 26

2.5 Πλατφόρμες ανάπτυξης 28

2.5.1 Ethereum 28

2.5.2 Hyperledger ... 30
2.5.3 Hyperledger Sawtooth ... 31
2.5.4 Hedera Hashgraph ... 32
2.5.5 Ripple ... 33
2.5.6 Quorum ... 34
2.5.7 OpenChain ... 35
2.5.8 Codra ... 36
2.5.9 EOS.IO ... 37
2.5.10 BigChainDB ... 37
3. Τομείς Χρήσης και Διαδεδομένες Εφαρμογές ... 38
3.1 Κυβερνήσεις και Δημόσιος Τομέας ... 38
3.1.1 E-Esthonia ... 38
3.1.2 Smart Dubai ... 38
3.2 Εφοδιαστική αλυσίδα ... 39
3.2.1 Treum ... 39
3.2.2 Η περίπτωση της Walmart ... 39
3.3 Νομικές Υπηρεσίες ... 40
3.3.1 OpenLaw. ... 40
3.4 Τράπεζες και χρηματοπιστωτικά Ιδρύματα ... 40
3.5 Φιλανθρωπικοί οργανισμοί ... 42
3.5.1 Bithope ... 42
3.5.2 Binance Charity ... 43
3.6 Προσωπικά Δεδομένων ... 43
3.6.1 Po.et ... 43
3.6.2 Bernstein ... 43
4. Προβληματισμοί ... 44
4.1 Κυβερνοεπιθέσεις στα Blockchain ... 44
4.2 Κακόβουλοι χρήστες ... 47
4.3 Το ερώτημα των επιχειρήσεων ... 47
4.4 Το ρίσκο της υιοθέτησης ... 48
5. Συμπεράσματα ... 49
Βιβλιογραφία ... 51

Συντομογραφίες & Ακρωνύμια

ABFT	Asynchronous Byzantine Fault Tolerance
API	Application Program Interface
BTC	Bitcoin
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DLT	Distributed Ledger Technology
DPOS	Delegated-Proof-of-Stake
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ETH	Ethereum
EVM	Ethereum Virtual Machine
HTTP	Hypertext Transfer Protocol
JSON	JavaScript Object Notation
PKC	Public-Key Cryptography
PoA	Proof-of-Authority
PoB	Proof-of-Burn
PoC	Proof-of-Capacity
PoET	Proof-of-Elapsed-Time
PoI	Proof-of-Identity
PoS	Proof-of-Space
PoW	Proof-of-Work
PoX	Proof-of-X
RSA	Rivest–Shamir–Adleman
SDK	Software Development Kit
SHA	Secure Hash Algorithms
UTXO	Unspent Transaction Output
MKO	Μη Κερδοσκοπικός Οργανισμός

Κατάλογος Πινάκων

Πίνακας 1. Παρουσίαση κατακερματισμού δεδομένων με χρήση του SHA-256, ο υπολογισμός έγινε στο https://xorbin.com/tools/sha256-hash-calculator 8
Πίνακας 2. Σύγκριση αλγορίθμων συναίνεσης 26
Πίνακας 3. Κρυπτογραφικοί αλγόριθμοι και κβαντικοί υπολογιστές 46

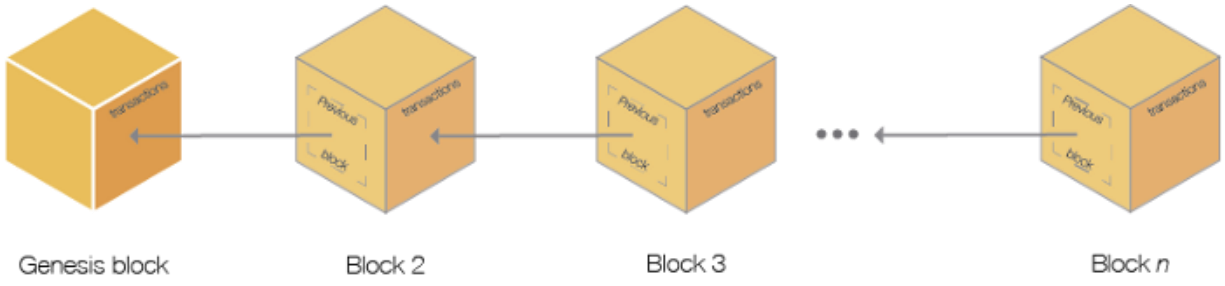
Κατάλογος Εικόνων

Εικόνα 1. BticoinWiki (χ.χ.). [Συστοιχία block ενός Blockchain]. Ανακτήθηκε 15 Σεπτεμβρίου 2020, από bitcoinwiki.org/wiki/Genesis_block *1*
Εικόνα 2. Network Encyclopedia (χ.χ). [Αλγόριθμος Κατακερματισμού]. Ανακτήθηκε 10 Αυγούστου 2020, από networkencyclopedia.com/hashing-algorithm *7*
Εικόνα 3. Kelly Robinson (2018). [Η διαδικασία της κρυπτογράφησης δημοσίου κλειδιού]. Ανακτήθηκε 10 Αυγούστου 2020, από https://www.twilio.com/blog/what-is-public-key-cryptography *10*
Εικόνα 4. Rahul (2018). [Διεύθυνση στο δίκτυο Bitcoin και QR code]. Ανακτήθηκε 9 Αυγούστου 2020, από https://unblock.net/bitcoin-address-work/ *12*
Εικόνα 5. Sonali Candel (2020). [Τα μέρη ενός block v, αριστερά το block v-1 και δεξιά το v+1] Ανακτήθηκε 9 Αυγούστου 2020, από https://www.researchgate.net/figure/The-structure-of-a-block-in-a-Blockchain_fig2_330832141 ..... *13*
Εικόνα 6. Marco Yuen (2014). [Δένδρο Merkle]. Ανακτήθηκε 27 Ιουλίου 2020, από http://www.marcoyuen.com/articles/2014/02/01/merkle-tree.html *14*
Εικόνα 7. Ethereum (χ.χ.). [Το λογότυπο της πλατφόρμας ανάπτυξης Ethereum]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.ethereum.org *28*
Εικόνα 8. Hyperledger (x.x) [Το λογότυπο της κοινότητας Hyperledger]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.hyperledger.org *30*
Εικόνα 9. Hyperledger (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Hyperledger Sawtooth]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από sawtooth.hyperledger.org *31*
Εικόνα 10. Hedera (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Hedera Hashgraph]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.hedera.com *32*
Εικόνα 11. Ripple (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Ripple]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.ripple.com *33*
Εικόνα 12. Consensys (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Quorum]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.goquorum.com *34*
Εικόνα 13. OpenChain (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης OpenChain]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.openchain.org *35*
Εικόνα 14. Corda (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης OpenChain]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.corda.net *36*
Εικόνα 15. EOS.IO (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης EOS.IO]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.eos.io *37*
Εικόνα 16. BigChainDB (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης BigChainDB]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.bigchaindb.com *37*
Εικόνα 17. [Απεικόνιση του αποκεντρωμένου καθολικού σε περιβάλλον τράπεζας]. (χ.χ). Ανακτήθηκε 3 Σεπτεμβρίου, από https://coinrevolution.com/what-is-a-distributed-ledger/ *42*

1. Εισαγωγή

1.1 Αντικείμενο πτυχιακής εργασίας

Το Blockchain, μια σχετικά καινούρια τεχνολογία, είναι μια ακολουθία από block η οποία σε αυτά κρατά και διαθέτει μια λίστα καταχωρήσεων - δεδομένων που αφορούν συναλλαγές μεταξύ χρηστών ενός τέτοιου δικτύου, σε ένα αποκεντρωμένο ψηφιακό δημόσιο σημειωματάριο (public ledger, DLT). Το σημειωματάριο αυτό ουσιαστικά αποτελεί το αρχείο κινήσεων του δικτύου. Είναι διαμοιρασμένο σε ένα δημόσιο ή ιδιωτικό peer-to-peer δίκτυο. Οι συναλλαγές επεκτείνονται και στην γενικότερη διακίνηση περιουσιακών στοιχείων. Στην *Εικόνα 1* φαίνεται ένα απλό παράδειγμα Blockchain. Στα block περιέχεται ένας κρυπτογραφημένος κωδικός κατακερματισμού. Κάθε block έχει σχέση άμεσα με το προηγούμενο block στην ακολουθία μέσω της τιμής κατακερματισμού του προηγούμενου block (ν-1), που βρίσκετε στην κεφαλή του block (ν). Το πρώτο block μια τέτοιας αλυσίδας λέγεται block πρώτης συναλλαγής (*genesis block*) και δεν υπάρχει κανένα άλλο πριν από αυτό.



Εικόνα 1. BticoinWiki (χ.χ.). [Συστοιχία block ενός Blockchain]. Ανακτήθηκε 15 Σεπτεμβρίου 2020, από bitcoinwiki.org/wiki/Genesis_block

Το βασικό κομμάτι πίσω από αυτό που ονομάζεται σήμερα Blockchain, ξεκίνησε πολλά χρόνια πριν. Στις αρχές του 1990, ο *Leslie Lamport* ανέπτυξε το πρωτόκολλο *Paxos* το οποίο παρουσιάστηκε αρκετά χρόνια αργότερα, το 1998, με τη δημοσίευση της έρευνας *The Part-Time Parliament* (Leslie, 1998) στο περιοδικό ACM Transactions on Computer Systems. Παράλληλα το 1991 ερευνητές εισήγαγαν για πρώτη φορά τη λογική μιας κρυπτογραφημένης αλυσίδας μέσω μιας ερευνητικής εργασίας *How to time-stamp a digital document* (Haber & Stornetta, 1991), στην οποία παρουσίαζαν μια πρακτική και πρωτότυπη λύση για την χρονοσήμανση εγγράφων κάνοντας την τροποποίησή τους αδύνατη. Μετά από χρόνια, το 2008 ένας Ιάπωνας (που δεν είναι γνωστό ακόμη για το αν πρόκειται για ένα άτομο ή για μια ομάδα ατόμων), δημοσίευσε μια ερευνητική εργασία *Bitcoin: A Peer to Peer Electronic Cash System* (Nakamoto, 2008). Στη συγκεκριμένη εργασία εισήγαγε για πρώτη φορά την τεχνολογία Blockchain για να δημιουργήσει το πρώτο ψηφιακό κρυπτονόμισμα, που είναι πλέον ευρέως γνωστό ως Bitcoin. Σύμφωνα με τον Pilkington (Pilkington, 2016), η εφεύρεση έγινε έχοντας ως βάση έναν κεντρικό διακομιστή (server) για την αποφυγή της διπλής σπατάλης (double-spending), ενός φαινομένου όπου η χρήση των ίδιων bitcoin γίνεται πάνω από μία φορά ταυτόχρονα. Παρόλα αυτά η συγκεκριμένη ιδέα με την χρήση διακομιστή απέτυχε καθώς δεν έδωσε λύσεις στα προβλήματα της διπλής σπατάλης, της ανωνυμίας και της αποκέντρωσης. Στη συνέχεια μεταξύ του 2011-2012 ξεκίνησε η χρήση κρυπτονομισμάτων σε πρακτικές εφαρμογές που είχαν σχέση με συναλλαγές.

1.2 Στόχοι της εργασίας

Οι στόχοι της εργασίας είναι η αναλυτική παρουσίαση και η εμβάθυνση στην τεχνολογία του Blockchain καθώς και σε όλα τα επιμέρους κομμάτια που απαρτίζουν ένα τέτοιο δίκτυο. Επιπλέον, η παρουσίαση του τρόπου δημιουργίας μιας εφαρμογής blockchain και η επίδραση που μπορεί να έχει στο σημερινό επιχειρηματικό κόσμο καθώς και όλα τα προβλήματα που μπορεί να δημιουργήσει μία υλοποίηση του.

1.3 Δομή της εργασίας

Κεφάλαιο 1ο : στο πρώτο κεφάλαιο παρουσιάζεται ο ορισμός, η ιστορία της δημιουργίας του blockchain, ο σκοπός της εργασίας, η διάρθρωσή της σε επιμέρους κεφάλαια.

Κεφάλαιο 2ο : στο δεύτερο κεφάλαιο γίνεται εισαγωγή στην τεχνολογία του Blockchain και παρουσίαση του τεχνολογικού της περιβάλλοντος (κατηγοριοποίηση, χαρακτηριστικά, τύποι, εκδόσεις, κατακερματισμός, κρυπτογραφία, διευθυνσιοδοτήσεις, ψηφιακές υπογραφές, δημόσια – ιδιωτικά κλειδιά κ.α.). Το κομμάτι των έξυπνων συμβολαίων αναφέρεται επίσης, μαζί με τα θετικά και αρνητικά που έχει η χρήση του. Επιπλέον αναφέρονται τα θετικά και αρνητικά της γενικής χρήσης του Blockchain. Παρουσιάζονται και συγκρίνονται διάφορα πρωτόκολλα συναίνεσης που χρησιμοποιούνται και τέλος αναφέρονται μερικές από τις πλατφόρμες που χρησιμοποιούνται για την ανάπτυξη εφαρμογών.

Κεφάλαιο 3ο : στο τρίτο κεφάλαιο παρουσιάζονται μερικοί από τους τομείς χρήσης της τεχνολογίας καθώς και αναλύονται εφαρμογές που χρησιμοποιούνται στους συγκεκριμένους κλάδους, παραθέτοντας τα ανάλογα παραδείγματα.

Κεφάλαιο 4ο : στο τέταρτο κεφάλαιο αναφέρονται προβληματισμοί σχετικά με την χρήση της τεχνολογίας. Είναι χρήσιμη η ανάπτυξη τέτοιων συστημάτων; Τί μορφές κυβερνοεπιθέσεων γίνονται; Πόσο ασφαλής είναι η τεχνολογία αυτή; όπως και πολλά άλλα ερωτήματα που διατυπώνονται και απαντώνται.

Κεφάλαιο 5ο : στο πέμπτο και τελευταίο κεφάλαιο γίνεται μια σύνοψη της εργασίας, σκέψεις για την κατάσταση που επικρατεί σήμερα με την χρήση της τεχνολογίας καθώς και για το τί πιθανώς πρόκειται να δούμε στο μέλλον να δημιουργείται από αυτή την τεχνολογία.

2. Ανάλυση Τεχνολογικού Περιβάλλοντος
2.1 Τεχνολογία Blockchain και αρχιτεκτονική
2.1.1 Τύπος Δικτύου

Ένα από τα πιο βασικά χαρακτηριστικά δικτύου Blockchain, είναι ο τύπος του. Υπάρχουν δύο τύποι δικτύου, ανάλογα με την άδεια ενεργειών που έχουν οι χρήστες. Αρχικά υπάρχουν τα δίκτυα που λειτουργούν χωρίς άδεια **(***permissionless***)** και με άδεια (*permissioned*). Ένας εύκολος και γρήγορος τρόπος για να καταλάβουμε την άμεση διαφορά μεταξύ τους, είναι να σκεφτούμε ένα απλό παράδειγμα, τη διαφορά χρήσης μεταξύ δύο τύπων δικτύων internet (εταιρικό–οικιακό). Τα Blockchain χωρίς άδεια είναι σαν το internet που διαθέτουμε στο σπίτι μας και έχουμε ελευθερία κινήσεων, ενώ τα Blockchain με άδεια είναι σαν το internet που διαθέτει μια επιχείρηση, όπου και υπάρχουν περιορισμοί για το τι επιτρέπεται να κάνουν οι χρήστες του. Επομένως τα δίκτυα με άδεια έχουν περιορισμούς στην ελευθερία κινήσεων των χρηστών. Ειδικότερα:

1. **Permissionless - Δημόσια:** Τα δίκτυα Blockchain που λειτουργούν χωρίς άδεια διαθέτουν ένα αποκεντρωμένο ψηφιακό δημόσιο σημειωματάριο το οποίο είναι ανοικτό σε κάθε χρήστη (miners, προγραμματιστές, χρήστες του δικτύου) να πραγματοποιήσει την κίνηση όπως ο ίδιος επιθυμεί, χωρίς να χρειάζεται την άδεια κάποια κεντρικής αρχής. Ο συγκεκριμένος τύπος blockchain συνήθως είναι *ανοιχτού κώδικα (open-source)* και ελεύθερος σε όποιον θέλει να το κατεβάσει και να συμμετάσχει. Λόγω της φύσης τους, οποιοσδήποτε μπορεί να δει το ιστορικό όλων των συναλλαγών του δικτύου καθώς και να προχωρήσει στην έκδοση block αυτοβούλως. Στα συγκεκριμένα δίκτυα καθώς η πρόσβαση είναι ελεύθερη, υπάρχει πιθανότητα να πραγματοποιηθούν απόπειρες αλλοίωσης των ήδη πραγματοποιημένων συναλλαγών ώστε συγκεκριμένοι χρήστες να επωφεληθούν. Για να μπορέσει να αποτραπεί ένα τέτοιο σενάριο έχουν δημιουργηθεί διάφορα πρωτόκολλα συναίνεσης, τα οποία μεταξύ των χρηστών δημιουργούν κανόνες για τη λειτουργεία του δικτύου.

2. **Permissioned - Ιδιωτικά:** Στα δίκτυα που λειτουργούν με άδεια, για την συμμετοχή χρηστών είναι απαραίτητη η παροχή άδειας από κάποια κεντρική αρχή, συγκεντρωμένη ή αποκεντρωμένη. Εφόσον πρόκειται για δίκτυα κλειστού τύπου υπάρχει η δυνατότητα να δίνονται δικαιώματα στο χρήστη για τις ενέργειες που μπορεί να κάνει. Δηλαδή, αν ο ίδιος μπορεί να δει τις συναλλαγές που έχουν γίνει, να δημιουργήσει καινούρια block ή και τα δύο. Όπως και στα δίκτυα χωρίς άδεια, έτσι και εδώ γίνεται χρήση πρωτοκόλλων συναίνεσης. Ωστόσο στη συγκεκριμένη περίπτωση τα πρωτόκολλα είναι διαφοροποιημένα και απαιτούν πολύ λιγότερη υπολογιστική ισχύ για την εκτέλεση τους. Μια ιδανική χρήση τέτοιου τύπου Blockchain είναι σε επιχειρήσεις που διαχειρίζονται ευαίσθητα δεδομένα και δεν θέλουν αυτά να είναι διαθέσιμα σε τρίτους. Τέλος και στο συγκεκριμένο τύπο δικτύου, αν και υπάρχει σχετική εμπιστοσύνη μεταξύ χρηστών, μπορεί να γίνουν κακόβουλες προσπάθειες για την αλλοίωση δεδομένων. Παρ' όλα αυτά καθώς πρόκειται για δίκτυο με όλους τους χρήστες του καταγεγραμμένους, η ανάκληση δικαιωμάτων και ο εντοπισμός τέτοιων αποπειρών είναι διαδικασία εύκολη και γρήγορη.

(Jayachandran, 2017)

2.1.2 Βασικά χαρακτηριστικά του Blockchain

Υπάρχουν τέσσερα βασικά χαρακτηριστικά τα οποία διαφοροποιούν το Blockchain από τα από τα έως τώρα γνωστά peer-to-peer δίκτυα.

1. ***Αποκέντρωση***: Στα έως τώρα γνωστά συστήματα συναλλαγών, για την πραγματοποίηση κάθε συναλλαγής, χρειάζεται έγκριση από κάποια κεντρική αρχή (πχ. στην περίπτωση της τράπεζας, από τον κεντρικό διακομιστή) για να πραγματοποιηθεί η ενέργεια αυτή. Αυτό έχει ως αποτέλεσμα το μεγαλύτερο κόστος λειτουργείας και την αύξηση κατά κόρον του μεγέθους υπολογιστικής ισχύος που χρειάζεται να έχει το σύστημα. Στα Blockchain η ύπαρξη κεντρικής αρχής δεν είναι απαραίτητη.
2. ***Ανθεκτικότητα***: Σε ένα τέτοιο δίκτυο είναι σχεδόν αδύνατη η διαγραφή ή η τροποποίηση συναλλαγών. Λόγω του τρόπου που είναι δομημένα τα block και με τα χαρακτηριστικά που διαθέτουν, οι μη έγκυρες εγγραφές - συναλλαγές εντοπίζονται απορρίπτονται από το δίκτυο.
3. ***Ανωνυμία***: Σε κάθε χρήστη ενός blockchain αντιστοιχεί μία τυχαία διεύθυνση, την οποία χρησιμοποιεί ο ίδιος για την πραγματοποίηση των συναλλαγών. Για την απόκτηση μιας τέτοιας διεύθυνσης δεν δίνονται προσωπικά δεδομένα του χρήστη όπως όνομα, επώνυμο, τηλέφωνο, διεύθυνση κτλ. πάρα μόνο η διεύθυνση email του, επιτυγχάνοντας έτσι την ανωνυμία.
4. ***Ελεγξιμότητα***: Το Blockchain, αποθηκεύει δεδομένα, σχετικά με το χρήστη λαμβάνοντας ως βάση το μοντέλο *Unspent Transaction Output (UTXO)*. Το συγκεκριμένο μοντέλο που χρησιμοποιείται από διάφορες πλατφόρμες όπως το Bitcoin, είναι το σύνολο των μη δαπανημένων νομισμάτων που παραμένουν στο λογαριασμό του χρήστη. Ένα παράδειγμα χρήσης τέτοιου παρόμοιου μοντέλου στον καθημερινό κόσμο είναι το λογιστικό υπόλοιπο που διαθέτει ένας λογαριασμός τράπεζας. Οποιαδήποτε κίνηση πραγματοποιείται θα πρέπει να συσχετίζεται άμεσα, μέσω δεδομένων, με την προηγουμένη. Όταν πραγματοποιείται συναλλαγή για να επικυρωθεί ακολουθείται μια διαδικασία κατά την οποία, καταγράφεται στο δίκτυο και η κατάσταση του υπολοίπου που πρόκειται να χρησιμοποιηθεί για την τρέχουσα συναλλαγή, αλλάζει από διαθέσιμη σε μη διαθέσιμη.

(Zheng, Xie, Dai, Chen, & Wang, 2017)

2.1.3 Αποκεντρωμένο καθολικό αρχείο

Βασικό χαρακτηριστικό της τεχνολογίας αυτής που αναφέρεται συχνά είναι το αποκεντρωμένο καθολικό αρχείο γνωστό και ως decentralized ledger ή DLT. Παρόμοια με τα άλλα βιβλία ιδιοκτησίας, που υπάρχουν παρά πολλά χρόνια και αναφέρουν τον ιδιοκτήτη αγαθών, έτσι και στο Blockchain πρόκειται για ένα αποκεντρωμένο βιβλίο που λειτουργεί σαν αρχείο για την καταγραφή οποιασδήποτε κίνησης πχ. συναλλαγή, εξόρυξη νέου block κ.α. , που γίνεται εντός του δικτύου και αφετέρου εμφανίζει τον ιδιοκτήτη κάθε περιουσιακού στοιχείου. Το συγκεκριμένο αρχείο μπορεί να είναι διαθέσιμο σε όλους τους συμμετέχοντες εάν είναι δημόσιο ενώ μπορεί να είναι ιδιωτικό όταν συγκεκριμένοι χρήστες έχουν πρόσβαση σε συγκεκριμένα δεδομένα του αρχείου. Το αρχείο αποθηκεύεται και διαμοιράζεται σε πολλούς χρήστες του δικτύου. Σε αυτό καταγράφονται μόνο οι έγκυρες και επιβεβαιωμένες συναλλαγές. Με την διατήρηση ενός τέτοιου

αρχείου εξασφαλίζεται αμεταβλητότητα, ιστορικότητα, διαφάνεια κινήσεων και λόγω του διαμοιρασμού, ασφάλεια στη διατήρηση των δεδομένων.

(R3, n.d.)

(Yaga & al., 2018)

2.1.4 Επιπλέον τύποι Blockchain

Εκτός από τα δίκτυα με ή χωρίς άδεια, τα Blockchain μπορούν να κατηγοριοποιηθούν και σε επιπλέον κατηγορίες βάση του τύπου λειτουργείας και διαμοιρασμού του καθολικού αρχείου συναλλαγών. Παραθέτονται μερικοί από τους βασικούς τύπους Blockchain:

- ***Δημόσια (public):*** στη συγκεκριμένη εκδοχή κάθε χρήστης μπορεί να λάβει μέρος εάν γίνει κόμβος. Τα δημόσια δίκτυα είναι και ανοιχτού κώδικα και όλος ο κώδικας του συστήματος υπάρχει στη διάθεση του καθενός. Τα σημειωματάρια δεν είναι στην κατοχή κανενός, είναι διαμοιρασμένα στους συμμετέχοντες και είναι διαθέσιμα να προβληθούν από όλους τους χρήστες του συστήματος.
- ***Ιδιωτικά (private):*** στη συγκεκριμένη εκδοχή μόνο χρήστες με άδεια μπορούν να λάβουν μέρος στο δίκτυο και να έχουν πρόσβαση σε δεδομένα. Τα σημειωματάρια είναι διαθέσιμα για όλους τους χρήστες του δικτύου.
- ***Ημι-ιδιωτικά (semi-private):*** στη συγκεκριμένη εκδοχή ένα μέρος του δικτύου, το ιδιωτικό είναι διαθέσιμο σε συγκεκριμένους χρήστες, ενώ το υπόλοιπο μέρος του – δημόσιο είναι διαθέσιμο στο ευρύ κοινό. Το ίδιο ισχύει και για το αρχείο συναλλαγών του.
- ***Sidechains:*** τα συγκεκριμένα Blockchain είναι γνωστά και ως πλευρικά. Αυτά δίνουν την δυνατότητα μετακίνησης νομισμάτων μεταξύ διαφορετικών υλοποιήσεων Blockchain. Σε αυτή την κατηγορία υπάρχουν δυο κατηγορίες: τα Blockchain μονής κατεύθυνσης όπου επιτρέπεται μόνο η μετακίνηση από το ένα Blockchain στο άλλο και τα αμφίδρομα Blockchain όπου επιτρέπεται η μετακίνηση νομισμάτων από και προς τις δύο πλευρές.
- ***Επιτρεπόμενο σημειωματάριο (permissioned ledger):*** στη συγκεκριμένη εκδοχή οι συμμετέχοντες έχουν εμπιστοσύνη μεταξύ τους και δεν χρειάζεται η χρήση κάποιου πρωτοκόλλου συναίνεσης πάρα μόνο ενός πρωτοκόλλου συμφωνίας.
- **Διαμοιρασμένο σημειωματάριο (distributed ledger)**: η συγκεκριμένη εκδοχή προσφέρει το αρχείο κινήσεων σε όλους τους συμμετέχοντες χωρίς περιορισμούς. Στη συγκεκριμένη κατηγορία είναι δυνατή και διατήρηση ενός τέτοιου αρχείου από ένα σύνολο οργανισμών που συμμετέχουν στο δίκτυο.
- ***Κοινόχρηστο σημειωματάριο (shared ledger):*** η συγκεκριμένη εκδοχή χρησιμοποιείται σε εφαρμογές ή βάσεις δεδομένων που απευθύνονται για χρήση από μεγάλο αριθμό χρηστών, είτε από το ευρύ κοινό, είτε από τους εργαζομένους μιας επιχείρησης όπου όλοι χρειάζονται να έχουν πρόσβαση σε παρόμοια δεδομένα.
- ***Fully Private of Proprietary Blockchains*****:** η συγκεκριμένη κατηγορία είναι χρήσιμη για την διακίνηση δεδομένων με την παροχή αυθεντικότητας. Χρήσεις που μπορούν να

γίνουν είναι για τη διακίνηση εξαιρετικά ευαίσθητων πληροφοριών μεταξύ τμημάτων της κυβέρνησης, κρατών, άκρως απόρρητων εργασιών κλπ.

- ***Tokenized Blockchains*:** τα συγκεκριμένα εμπίπτουν στην κατηγορία παραγωγής κρυπτονομισμάτων χρησιμοποιώντας την τεχνική της εξόρυξης ή της αρχικής διανομής (initial distribution).
- ***Tokenless Blockchains*:** η συγκεκριμένη κατηγορία διαφέρει κατά πολύ με τι έως τώρα γνωστές, εφόσον πρόκειται για εξαιρετικά ιδιωτικό δίκτυο και χρησιμοποιείται αποκλειστικά για τη μεταφορά δεδομένων μεταξύ χρηστών όπου υπάρχει απόλυτη εμπιστοσύνη.

(Sarmah, 2018)

2.1.5 Εκδόσεις του Blockchain

Έως σήμερα το Blockchain έχει 4 εκδόσεις, από την 1.0 έως την 4.0. Κάθε μία από τις εκδόσεις έχει και διαφορετικό φάσμα χρήσεων και απαιτήσεις. Με την πάροδο των εκδόσεων, στο Blockchain προστίθενται επιπλέον λειτουργείες και βελτιστοποιείται η κατανάλωση ενέργειας και η ανάγκη ύπαρξης μεγάλης υπολογιστικής ισχύος για την άρτια λειτουργεία των δικτύων.

Blockchain 1.0, Κρυπτονομίσματα

Η πρώτη έκδοση Blockchain χρησιμοποιείται για κρυπτονομίσματα και πρωτοεμφανίστηκε το 2008 με τη δημιουργία του Bitcoin. Όπως και το Bitcoin έτσι και όλα τα υπόλοιπα νομίσματα αντίστοιχης τεχνολογίας χρησιμοποιούν την συγκεκριμένη έκδοση. Η συγκεκριμένη έκδοση έφερε για πρώτη φορά ευρέως στον τεχνολογικό κόσμο τη λογική κατανεμημένων καθολικών αρχείων συναλλαγών.

Blockchain 2.0, Έξυπνα Συμβόλαια

Η δεύτερη έκδοση δημιουργήθηκε όταν προγραμματιστές κατάλαβαν ότι το Blockchain μπορεί να έχει εφαρμογές και πέρα από τον κόσμο των συναλλαγών. Τα έξυπνα συμβόλαια χρησιμοποιούνται στον χρηματοοικονομικό κλάδο καθώς και στην εφοδιαστική αλυσίδα. Στη συγκεκριμένη έκδοση πρωτοεμφανίστηκαν και τα έξυπνα συμβόλαια (Smart Contracts), τα οποία μπορούν να οριστούν ως ένας τρόπος ελέγχου μεταξύ δύο μερών (πχ. συμβαλλόμενος – αντισυμβαλλόμενος.). Κατά την εκτέλεση τέτοιων συμβολαίων επιβεβαιώνεται η αποστολή - πραγματοποίηση προϊόντων - υπηρεσιών κατά τη διάρκεια πραγματοποίησης συναλλαγής μεταξύ των δύο μερών.

Blockchain 3.0, Αποκεντρωμένες εφαρμογές, DApps

Με την τρίτη έκδοση της τεχνολογίας εισέρχονται οι αποκεντρωμένες εφαρμογές. Αυτή η έκδοση προσφέρει μεγάλη επεκτασιμότητα της εφαρμογής και περισσότερη ασφάλεια σε σύγκριση με τις προγενέστερες εκδόσεις. Ουσιαστικά προσπαθεί να επιλύσει όσα προβλήματα ήταν ορατά στις προηγούμενες εκδόσεις, σχετικά με την χρήση σε ένα σχετικά μικρό κλάδο επιχειρήσεων καθώς και με την μείωση σε υπολογιστική και ενεργειακή ισχύ που χρειάζεται το Blockchain για να

λειτουργεί. Πλέον το Blockchain εισέρχεται και παρέχει λύσεις σε ένα μεγάλο μέρος του επιχειρηματικού κλάδου όπως η υγεία, ο νομικός κλάδος, οι κυβερνήσεις κλπ.

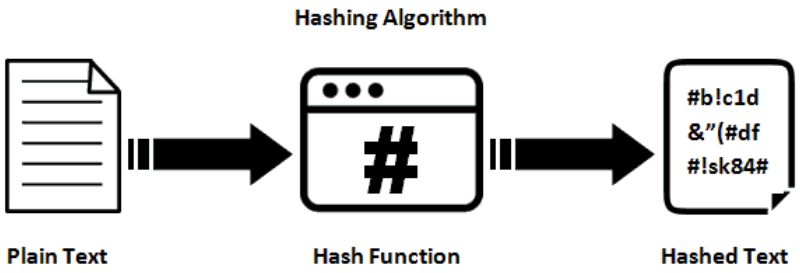
Blockchain 4.0 - Διείσδυση του Blockchain στη γενικότερη βιομηχανία

Η τέταρτη και τελευταία έκδοση της τεχνολογίας έως σήμερα έρχεται να φέρει την δυνατότητα παροχής λύσεων, που πλέον κάνουν το Blockchain χρησιμοποιήσιμο σε επιχειρηματικές απαιτήσεις. Πλέον το Blockchain μπορεί να φέρει λύσεις ακόμη και σε αυτοματισμούς, συστήματα διαχείρισης επιχειρησιακών πόρων (*ERP*) κ.α. Με αυτή την έκδοση το Blockchain μπορεί να χρησιμοποιηθεί και να λειτουργήσει για την καλυτέρευση διαχείριση εφοδιαστικής αλυσίδας, για τη ροή εργασιών, για χρηματοοικονομικές συναλλαγές, για συλλογή δεδομένων Internet of Things κ.α.

(Unibright.io, 2017)

2.1.6 Κρυπτογραφημένες συναρτήσεις κατακερματισμού

Ίσως και το πιο σημαντικό μέρος της τεχνολογίας Blockchain που το διαφοροποιεί κατά κόρον από τα υπόλοιπα γνωστά δίκτυα, είναι η χρήση κρυπτογραφημένων συναρτήσεων κατακερματισμού (*hash functions*). Κατακερματισμός (*hashing*) είναι μια μέθοδος εφαρμογής συναρτήσεων σε δεδομένα, κατά την οποία από μια οποιαδήποτε είσοδο (input) έχουμε μία και μοναδική έξοδο (*output*) δεδομένων. Στο κόσμο της κρυπτογραφίας η συγκεκριμένη τεχνική είναι γνωστή ως σύνοψη μηνύματος (*message digest*). Μία απλή απεικόνιση λειτουργείας της συγκεκριμένης συνάρτησης παρουσιάζεται στην *Εικόνα 2*.



Εικόνα 2. Network Encyclopedia (χ.χ). [Αλγόριθμος Κατακερματισμού]. Ανακτήθηκε 10 Αυγούστου 2020, από networkencyclopedia.com/hashing-algorithm

Για ασφάλεια, οι συγκεκριμένοι αλγόριθμοι είναι μονής κατεύθυνσης, δηλαδή μπορούμε να πηγαίνουμε μόνο από τα αριστερά στα δεξιά, μόνο από μία είσοδο σε μία έξοδο. Το αντίθετο είναι σχεδόν υπολογιστικά ανέφικτο να συμβεί στις μέρες μας. Σύμφωνα με πολλές θεωρίες κρυπτογραφίας , οι συναρτήσεις κατακερματισμού h: από μια είσοδο X σε μια έξοδο Y έχουν τις τρείς παρακάτω ιδιότητες, οι οποίες είναι και σημαντικές για την διατήρηση της ασφάλειας του συστήματος που τους χρησιμοποιεί.

1. Με την ύπαρξη συνάρτησης κατακερματισμού όπου h και y που να ανήκουν στο Y, πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί x, τέτοιο ώστε h(x) = y, πρώτη αντίσταση σε σύγκρουση (*preimage resistance*).
2. Με την ύπαρξη συνάρτησης κατακερματισμού όπου h και x που να ανήκουν στο X, πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί x΄ τέτοιο h(x΄) = h(x), δεύτερη αντίσταση σε σύγκρουση (*second preimage resistance*).
3. Με την ύπαρξη συνάρτησης κατακερματισμού h, πρέπει να είναι υπολογιστικά αδύνατο να βρεθούν x, x' που να ανήκουν στο X, ώστε h(x) = h(x΄), ισχυρή αντίσταση σε σύγκρουση (*strong collision resistance*).

Πλέον υπάρχουν πολλοί αλγόριθμοι κατακερματισμού, όπως ο *Message Direct* (*MD, MD2, MD4, MD5 & MD6*), ο *RIPEMD*(*RIPEMD, RIPEMD-128, RIPEMD-256 & RIPEMD-160*) κ.α. Ωστόσο, ο πιο διαδεδομένος αλγόριθμος κατακερματισμού στο χώρο του Blockchain είναι η οικογένεια των *Secure Hash Algorithm* (*SHA-0, SHA-1, SHA-2 και SHA-3*) και συγκεκριμένα ο αλγόριθμος της οικογένειας *SHA-2*, ο 256 bits (*SHA-256*). Πολλοί υπολογιστές υποστηρίζουν το συγκεκριμένο αλγόριθμο κάνοντας εύκολα και γρήγορα την εκτέλεσή του.

Η συνάρτηση *SHA-256* στην έξοδό της εμφανίζει ένα 64άρων χαρακτήρων αλφαριθμητικό στο δεκαεξαδικό σύστημα αρίθμησης (0 – F), το οποίο είναι μοναδικό για κάθε διαφορετική είσοδο δεδομένων. Όπως φαίνεται και στον *Πίνακα 1* που ακολουθεί αν και χρησιμοποιήθηκε η ίδια ακριβώς λέξη, με τη μόνη διαφορά ένα γράμμα που έγινε μικρό από κεφάλαιο, παρατηρούμε ότι τα δυο αλφαριθμητικά δεν έχουν καμία σχέση μεταξύ τους και οπτικά δεν φαίνεται η παραμικρή σχέση τους.

Πίνακας 1. *Παρουσίαση κατακερματισμού δεδομένων με χρήση του SHA-256, ο υπολογισμός έγινε στο* https://xorbin.com/tools/sha256-hash-calculator

Είσοδος	Κατακερματισμένη τιμή με χρήση του αλγορίθμου SHA-256
Καλησπέρα	6e67dfcd889376ea50d836a05b56de5f30e820d2dfdba192fa8c5373da1365d1
καλησπέρα	9d6e3528137f044778c6bb9407bf0418b60be6e45f055c4afc17c7996416af2b

Οι συναρτήσεις κατακερματισμού εκτός από την γενικότερη κρυπτογράφηση δεδομένων, ειδικεύονται και για επιμέρους διαδικασίες για τη λειτουργεία ενός blockchain.

- Για διαδικασίες διευθυνσιοδοτήσεων χρηστών.
- Για τη δημιουργία μοναδικών αναγνωριστικών, ώστε να είναι μοναδικό κάθε block και να διαχωρίζεται εύκολα.
- Για τη διασφάλιση των δεδομένων που υπάρχουν σε ένα block, στο κυρίως μέρος του και στην κεφαλή του.

(Yaga & al., 2018)

2.1.7 Σετ κλειδιών, ψηφιακή υπογραφή και κρυπτογράφησή της

Στα Blockchain, σε κάθε χρήστη αντιστοιχεί ένα ζευγάρι ψηφιακών κλειδιών (set of keys), ένα **ιδιωτικό** και ένα **δημόσιο**. Καθένα από αυτά προορίζεται και έχει διαφορετική χρήση. Αν και στο ζευγάρι κλειδιών, τα δύο κλειδιά οπτικά δεν μοιάζουν, συνδέονται μεταξύ τους μέσω μαθηματικών αλγορίθμων. Οι δύο τύποι κλειδιών μαζί με τα χαρακτηριστικά τους αναλύονται παρακάτω.

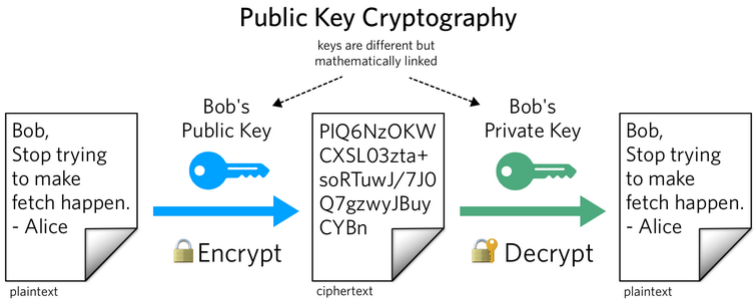
1. **Ιδιωτικό κλειδί (private key):** όπως λέει και το όνομά του είναι ιδιωτικό και δεν θα πρέπει να μοιράζεται, καθώς αυτό χρησιμοποιείται για την υπογραφή συναλλαγών. Σε περίπτωση διαμοιρασμού του ιδιωτικού κλειδιού**,** δεδομένα και γενικά περιουσιακά στοιχειά τα οποία διαχειρίζονται από αυτά τα κλειδιά, μπορούν να μοιραστούν σε χρήστες που δεν πρέπει να έχουν σε αυτά πρόσβαση.
2. **Δημόσιο κλειδί (public key):** μπορεί να χρησιμοποιηθεί μεταξύ δύο χρηστών, για την επιβεβαίωση ότι τα δεδομένα που διακινήθηκαν μεταξύ τους είναι αυθεντικά και δεν έχουν αλλοιωθεί στο μεσοδιάστημα από κάποιον τρίτο.

Όλες οι ψηφιακές συναλλαγές που έχουν υπογραφεί και εγκριθεί, μεταδίδονται σε ολόκληρο το δίκτυο και καταγράφονται στο καθολικό αρχείο συναλλαγών. Ο αλγόριθμος που χρησιμοποιείται στα περισσότερα δίκτυα Blockchain για την παραπάνω διαδικασία, είναι η **ψηφιακή υπογραφή ελλειπτικής καμπύλης** (*Elliptic Curve Digital Signature Algorithm* ή *ECDSA*). Ο συγκεκριμένος αλγόριθμος έχει ως βάση τον αλγόριθμο **ψηφιακής υπογραφής** (*Digital Signature Algorithm ή DSA*) που χρησιμοποιεί κλειδιά που προέρχονται από την **κρυπτογραφία ελλειπτικών καμπυλών** (*Elliptic Curve Cryptography ή ECC*). Υπάρχουν πολλοί αλγόριθμοι που βασίζονται πάνω στο μοντέλο του *ECC*, ωστόσο ο αλγόριθμος ECDSA σε σύγκριση με άλλους, είναι πιο αποδοτικός και παράλληλα γρήγορος καθώς για την παροχή ισοδύναμης ασφάλειας χρειάζεται μικρότερα κλειδιά σε μήκος χαρακτήρων.

(Yaga & al., 2018)

2.1.8 Κρυπτογράφηση Δημόσιου Κλειδιού (PKC)

Η ιδέα της κρυπτογράφησης δημόσιου κλειδιού (*Public Key Cryptography ή PKC*) είναι παρόμοια με αυτή των συναρτήσεων κατακερματισμού που προαναφέρθηκαν. Και σε αυτή την περίπτωση πρόκειται για μια διαδικασία μονής κατεύθυνσης, όπου από μία εισαγωγή δεδομένων καταλήγουμε σε μία μοναδική έξοδο, η αντίστροφη διαδικασία και εδώ είναι υπολογιστικά αδύνατη να συμβεί. Η κρυπτογράφηση *PKC* χρησιμοποίει ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό. Για την αποστολή δεδομένων μεταξύ χρηστών, ο αποστολέας υπογράφει - κρυπτογραφεί τα δεδομένα με τη χρήση του ιδιωτικού του κλειδιού. Ο παραλήπτης από την άλλη με τη χρήση του δημόσιου κλειδιού του αποστολέα εγκρίνει την εγκυρότητα των δεδομένων και αποκρυπτογραφεί τα δεδομένα που του στάλθηκαν.



Εικόνα 3. Kelly Robinson *(2018).* [Η διαδικασία της κρυπτογράφησης δημοσίου κλειδιού]. Ανακτήθηκε 10 Αυγούστου 2020, από *https://www.twilio.com/blog/what-is-public-key-cryptography*

Η πορεία των υπολογισμών και η διαδικασία *PKC*, παρουσιάζεται με ένα απλό και εύκολο στην κατανόηση διάγραμμα στην *Εικόνα 3***.** Στο διάγραμμα υπάρχουν δύο χρήστες ο Bob και η Alice. Ο Bob στέλνει ένα στην Alice δεδομένα κειμένου. Με την χρήση των κλειδιών του Bob, το κείμενο κρυπτογραφείται κατάλληλα σε κείμενο μη κατανοητό, έτσι ώστε και αν υποκλαπεί κατά τη διαδικασία της μεταφοράς, να μην μπορεί να αποκαλύψει στον τρίτο τί ακριβώς αφορούν τα δεδομένα που κατάφερε και υπέκλεψε. Στην συνέχεια το αρχείο διακινείται μέσω του peer-to-peer δικτύου και τελικά καταλήγει στην Alice. Τέλος τα δεδομένα έχουν φτάσει στην Alice η οποία πλέον αποκρυπτογραφεί το κείμενο με τη χρήση του ιδιωτικού κλειδιού του Bob και η Alice έχει πλέον την αρχική κατάσταση του κειμένου.

(Robinson, 2018)

2.1.9 Διαχείριση του Ιδιωτικού Κλειδιού

Τα ιδιωτικά κλειδιά είναι χαρακτηριστικά πολύ απαραίτητα σε ένα δίκτυο καθώς και για τη διαχείριση της ψηφιακής περιουσίας του χρήστη. Οι χρήστες που κατέχουν ιδιωτικά κλειδιά θα πρέπει να τα αποθηκεύουν σε ασφαλή μέρη με κάποιο τρόπο ώστε να είναι εύκολη και άμεση η ανάκτησή τους. Όταν αναφερόμαστε σε ιδιωτικά κλειδιά, θα πρέπει να γνωρίζουμε ότι αφορούν ένα αλφαριθμητικό μεγάλου μήκους, το οποίο χαρακτηριστικό μεταβάλλεται ανάλογα με τις ιδιότητες που έχουν καθοριστεί στο εκάστοτε δίκτυο. Καθώς η διαχείρισή τους είναι δύσκολη, ειδικά αν οι χρήστες κρατάνε μεγάλο όγκο κλειδιών, έχουν δημιουργηθεί ψηφιακά πορτοφόλια (*wallets*). Η βασική τους χρήση είναι η αποθήκευση και διαχείριση ιδιωτικών κλειδιών. Ωστόσο καθώς συνεχώς μπαίνουν στα Blockchain νέες δυνατότητες, δημιουργούνται νέα λογισμικά που επιτρέπουν την εξ ολοκλήρου διαχείριση ψηφιακής περιουσίας από ένα και μόνο σημείο.

Οι χρήστες θα πρέπει ανά πάσα στιγμή να γνωρίζουν τα κλειδιά τους, καθώς σε περίπτωση απώλειας, αυτομάτως χάνουν και την όποια ψηφιακή περιουσία συνοδεύουν αυτά. Σε περίπτωση που συμβεί κάτι τέτοιο, η ανάκτησή τους είναι αδύνατη, επειδή είναι και αδύνατη η δημιουργία παρομοίου κλειδιού στο ίδιο δίκτυο. Οι χρήστες επιπλέον θα πρέπει να προσέχουν και για το που καταχωρούν – με ποιους μοιράζονται τα κλειδιά τους. Σε περίπτωση που κάποιος τρίτος κατέχει

ιδιωτικά κλειδιά ενός ατόμου, μπορεί να μεταφέρει και την περιουσία που συνοδεύουν αυτά όπου επιθυμεί. Η συγκεκριμένη ενέργεια είναι μη αναστρέψιμη.

Καθώς πρόκειται για αρκετά σημαντικό χαρακτηριστικό, οι χρήστες κάνουν χρήση ιδιαίτερα εξελιγμένων εφαρμογών και συστημάτων για την ασφαλή αποθήκευση των κλειδιών τους, καθώς και υψηλού επιπέδου κρυπτογραφίας.

(Yaga & al., 2018)

2.1.10 Κόμβοι (*Nodes*) και Υπερκόμβοι (*Masternodes*)

Στα δίκτυα Blockchain όταν ένας miner προσπαθεί να προσθέσει ένα block στην αλυσίδα, η διαδικασία αυτή μεταδίδεται σε όλους τους κόμβους του δικτύου. Οι κόμβοι από την πλευρά τους ελέγχουν από τα δεδομένα που λαμβάνουν την εγκυρότητα της συναλλαγής που προσπαθεί να προστεθεί στο δίκτυο και ανάλογα με την απόφαση που θα πάρουν, είτε δέχονται το block και το προσθέτουν στην αλυσίδα, είτε το απορρίπτουν τελείως. Οι λειτουργίες που εκτελούν οι κόμβοι αφορούν τα παρακάτω.

1. Έλεγχός εγκυρότητας των block συναλλαγών και αποδοχή ή απόρριψη αυτών.
2. Διαχείριση του ιστορικού του δικτύου μέσω της ορθής αποθήκευσης των block.
3. Διαμοιρασμός του αρχείου συναλλαγών του δικτύου στους υπεύθυνους κόμβους για λόγους ενημέρωσης και διατήρησης ιστορικότητας.

Οι κόμβοι μπορούν να είναι δύο ειδών βάση του τρόπου που λειτουργούν στο δίκτυο. Υπάρχουν οι συνδεμένοι (online) που λαμβάνουν τις κινήσεις του δικτύου σε σχεδόν πραγματικό χρόνο και από την άλλη υπάρχουν και οι κόμβοι εκτός σύνδεσης (offline) που δεν λειτουργούν συνεχώς και κάθε φορά που συνδέονται - εισέρχονται στο δίκτυο, θα πρέπει να συγχρονίσουν και να λάβουν όλες τις κινήσεις που πραγματοποιήθηκαν τον καιρό που έμειναν εκτός σύνδεσης.

Ένα δίκτυο Blockchain θεωρητικά μπορεί να εκτελείται από έναν και μόνο κόμβο. Επειδή ο κόμβος κατέχει τα δεδομένα όλου του Blockchain, η ύπαρξη ενός μόνο κόμβου σε περίπτωση εμφάνισης προβλημάτων όπως διακοπές ρεύματος, κυβερνοεπιθέσεις και τυχαία σφάλματα συστήματος θέτει σε κίνδυνο την λειτουργεία ολόκληρου του δικτύου. Τα δεδομένα, όσο περισσότερο διαμοιρασμένα είναι σε περισσότερους κόμβους, τόσο μεγαλύτερη ασφάλεια υπάρχει για την αντιμετώπιση των προηγούμενων προβλημάτων. Οποιοσδήποτε χρήστης, εάν του παρέχεται η ανάλογη άδεια που πιθανώς να χρειάζεται, μπορεί να εκτελέσει έναν κόμβο πολύ απλά με την λήψη του ιστορικού συναλλαγών ενός Blockchain και χωρίς να χρειάζεται να διαθέτει εξιδεικευμένα συστήματα ή μεγάλη υπολογιστική ισχύ.

Εκτός από τους κόμβους, σε μερικά Blockchain υπάρχουν και οι υπερκόμβοι. Αυτά εκτός από τις τρείς συγκεκριμένες λειτουργείες των κόμβων μπορούν να επιτελέσουν και επιπλέον λειτουργίες ανάλογα με τα απαιτούμενα κάθε υλοποίησης. Οι επιπρόσθετες λειτουργίες ποικίλουν και μπορούν να αφορούν στην εκτέλεση πρωτοκόλλων, στον έλεγχο τήρησης των κανόνων που έχουν θεσπιστεί στο δίκτυο κ.α. Εν αντιθέσει με τους απλούς κόμβους, οι υπερκόμβοι πρέπει να τρέχουν συνεχώς

χωρίς διακοπές. Τέλος οι υπερκόμβοι δεν μπορούν να εκτελούνται από τον οποιονδήποτε, για λόγους ασφαλείας και κόστους. Για την απόκτηση ενός τέτοιου κόμβου συνήθως απαιτείται η κατάθεση ενός σχετικά μεγάλου ποσού ως εγγύηση στους διαχειριστές του εκάστοτε Blockchain.

(Nodes, n.d.)

2.1.11 Διευθυνσιοδοτήσεις στα δίκτυα Blockchain

Έχει αναφερθεί ότι στους χρήστες μερικών δικτυών Blockchain αντιστοιχεί μία διεύθυνση η οποία είναι ένα αλφαριθμητικό το οποίο προκύπτει από το δημόσιο κλειδί του χρήστη, με ακόμη κάποια επιπλέον στοιχεία (π.χ. αριθμός της έκδοσης, ειδικοί αλγόριθμοι κ.α.) χρησιμοποιώντας αλγορίθμους κατακερματισμού. Οι διευθύνσεις είναι δεδομένα το οποία είναι δημόσια. Στις περισσότερες υλοποιήσεις Blockchain που υπάρχουν σήμερα, στο αρχείο καθώς και στα δεδομένα του block συναλλαγής καταγράφονται και αποθηκεύονται ο αποστολέας και ο αποδέκτης της εκάστοτε συναλλαγής.

Ο τρόπος που γίνεται η διευθυνσιοδότηση διαφέρει, ανάλογα με τον τρόπο που έχουν επιλέξει οι δημιουργοί της πλατφόρμας να γίνεται η διαδικασία. Στα δίκτυα που λειτουργούν χωρίς την ανάγκη άδειας και είναι ελεύθερα, οι χρήστες μπορούν να δημιουργήσουν άπειρα προφίλ και άπειρα κλειδιά με αποτέλεσμα ο κάθε χρήστης να έχει τη δυνατότητα να δημιουργεί όσες διευθύνσεις επιθυμεί. Από την άλλη στα δίκτυα που χρειάζεται άδεια για την συμμετοχή, κάθε χρήστες έχει μία ή το πολύ έναν μικρό αριθμό διευθύνσεων.

Ένα παράδειγμα διεύθυνσης (ενός πορτοφολιού Bitcoin(BTC)) βρίσκεται στην *Εικόνα 4* όπου και βλέπουμε την αλφαριθμητική διεύθυνση. Η τελευταία πολλές φορές συνοδεύεται και από ένα QR code που αντιστοιχεί στη διεύθυνση το οποίο μπορεί να χρησιμοποιηθεί γρήγορα για την εύκολη ανάκτηση της διεύθυνσης από ένα smartphone ή από ένα web-app.

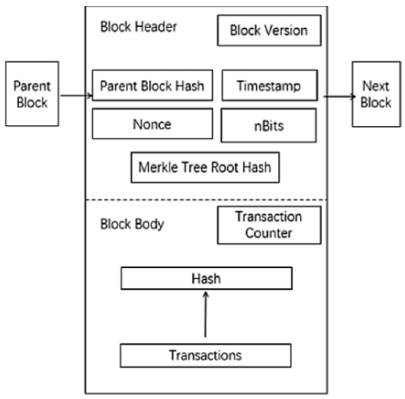
Εικόνα 4. Rahul *(2018).* [Διεύθυνση στο δίκτυο Bitcoin και QR code]. Ανακτήθηκε 9 Αυγούστου 2020, από *https://unblock.net/bitcoin-address-work/*

Η χρήση των διευθύνσεων πέρα από τις υλοποιήσεις νομισμάτων και συναλλαγών (Bitcoin, Ethereum κλπ.) αφορά και υλοποιήσεις του Blockchain με τη χρήση των έξυπνων συμβολαίων για την ανταλλαγή περιουσιακών στοιχείων μεταξύ συμβαλλόμενων.

(Yaga & al., 2018)

2.1.12 Block και τεχνολογικά χαρακτηριστικά

Όπως αναφέρθηκε, όταν γίνεται ένα είδος συναλλαγής στα δίκτυα Blockchain, ένα χρήστης αποστέλλει το αίτημά του στους κόμβους, οι οποίοι με τη σειρά τους ελέγχουν τη συναλλαγή και πράττουν ανάλογα. Οι συναλλαγές προστίθενται στο δίκτυο όταν ένας κόμβος δημοσιεύει στο δίκτυο ένα block. Το Blockchain αποτελείται από πολλά block τα οποία βρίσκονται σε μία σειρά και δημιουργούν μία αλυσίδα. Κάθε block μπορεί να χωριστεί σε 2 μέρη, την κεφαλή (*header*) που διατηρεί τα μεταδεδομένα της συναλλαγής και το κυρίως μέρος (*body*) που διατηρεί επιπλέον στοιχεία για της συναλλαγές που έχουν πραγματοποιηθεί. Τα χαρακτηριστικά του block μπορούν να διαφοροποιηθούν ανάλογα με τις δυνατότητες που χρειάζεται να διαθέτει κάθε δίκτυο. Ακολουθεί στην *Εικόνα 5*, παράδειγμα με την παρουσίαση των χαρακτηριστικών ενός block που υπάρχει στο κρυπτονόμισμα Bitcoin.



Εικόνα 5. Sonali Candel (2020). [Τα μέρη ενός block ν, αριστερά το block ν-1 και δεξιά το ν+1] Ανακτήθηκε 9 Αυγούστου 2020, από https://www.researchgate.net/figure/The-structure-of-a-block-in-a-Blockchain_fig2_330832141

Η **κεφαλή** αποτελείται από 6 χαρακτηριστικά:

1. **Έκδοση Block** (block version), η οποία επισημαίνει το σύνολο κανόνων που θα πρέπει να ακολουθηθούν και έχουν οριστεί κατά τη δημιουργία του δικτύου.
2. **Κατακερματισμένη τιμή ρίζας δένδρου Merkle (***Merkle tree root hash***)**, η οποία είναι η τιμή κατακερματισμού όλων των συναλλαγών που υπάρχουν σε ένα block.
3. **Χρονοσήμανση** (*Timestamp***)**, που είναι ο χρόνος που δημιουργήθηκε ένα block εκφρασμένος σε δευτερόλεπτα. Στα block χρησιμοποιείται ο τρόπος υπολογισμού του χρόνου των συστημάτων UNIX όπου κάθε δευτερόλεπτο είναι ένας ακέραιος και μοναδικός αριθμός (*Unix Epoch Time*). Ως σημείο μηδέν έχει οριστεί η 01/01/1970 00:00:00 οπού η προηγούμενη τιμή είναι η 0 και για κάθε δευτερόλεπτο που περνάει, η τιμή αυτή αυξάνεται κατά 1.
4. **nBits**, κωδικοποιημένη τιμή που αναφέρεται στον στόχο κατακερματισμού, που υπάρχει στην κεφαλή του block. Ο στόχος είναι μια τιμή 256-bit και αντιστρόφως ανάλογος με τη δυσκολία.
5. **Nonce**, ένας τυχαίος ακέραιος αριθμός ο οποίος όταν προστίθεται σε ένα κατακερματισμένο block θα πρέπει να συμφωνεί με το επίπεδο δυσκολίας. Συναντάτε

συνήθως σε Blockchain που βασίζονται στο *Proof-of-Work* πρωτόκολλο συναίνεσης και λαμβάνει τιμές από 0 έως 2^{32} .

6. **Parent block hash**, τιμή κατακερματισμού 256-bit όπου έχει σχέση με την τιμή του προηγούμενου block της σειράς, από εκεί προκύπτει και η άμεσα σύνδεση των block μεταξύ τους.

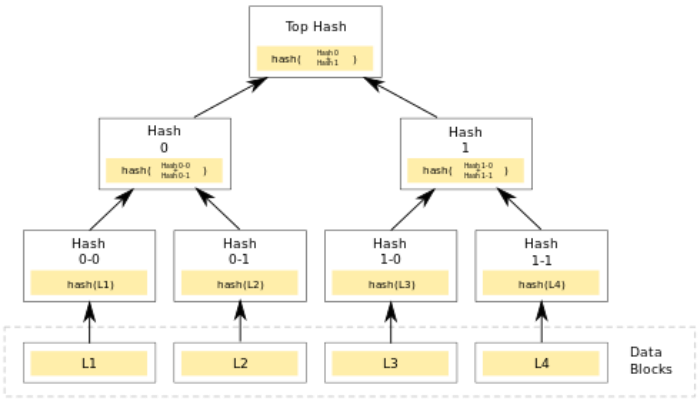
Το **κυρίως μέρος** περιέχει όλες τις επιβεβαιωμένες συναλλαγές που σχετίζονται με το block. Επιπλέον ανάλογα και με την κάθε υλοποίηση του Blockchain μπορεί να περιέχει και επιπρόσθετες πληροφορίες που χαρακτηρίζονται ως απαραίτητες. Ο μέγιστος αριθμός συναλλαγών που ένα block μπορεί να αποθηκεύσει εξαρτάται από το μέγεθος του ίδιου, των συναλλαγών καθώς και του ορίου που έχει οριστεί κατά την κατασκευή του Blockchain από τους δημιουργούς.

(Zheng, Xie, Dai, Chen, & Wang, 2017)

2.1.13 Δένδρα Merkle

Τα δένδρα Merkle που σχετίζονται με κάθε μπλοκ που υπάρχει στην συστοιχία, αποτελούν σημαντικό χαρακτηριστικό για την ακεραιότητα δεδομένων του τομέα της κρυπτογραφίας και γενικότερα της πληροφορικής. Για την κατανόηση των δένδρων θα παρουσιαστεί ένα παράδειγμα δένδρου που θα περιγράφει τη σχέση που έχουν μεταξύ τους τα επιμέρους κομμάτια του, από πάνω προς τα κάτω, από το φύλλο, στο κλαδί και τέλος στη ρίζα.

Μέσω αυτών των δένδρων, για το παράδειγμα του δένδρου, κάθε κόμβος – φύλλο (leaf) περιέχει ένα σύνολο δεδομένων. Πίσω από κάθε τέτοιο φύλλο υπάρχει ένας γονικός κόμβος (parent) – κλαδί, ο οποίος περιέχει τα δεδομένα των προηγούμενων κόμβων σε κατακερματισμένη μορφή. Συνήθως στα δένδρα που υπάρχουν, επιτρέπεται στους κόμβους να έχουν έως 2 παιδιά - φύλλα. Στην αρχή του δένδρου υπάρχει η ρίζα (root), η οποία περιλαμβάνει το σύνολο των κατακερματισμένων δεδομένων που υπάρχουν ακριβώς πάνω από αυτή και συνοψίζουν την συνολική εικόνα του δένδρου που ακολουθεί.



Εικόνα 6. Marco Yuen (2014). [Δένδρο Merkle]. Ανακτήθηκε 27 Ιουλίου 2020, από http://www.marcoyuen.com/articles/2014/02/01/merkle-tree.html

Σε peer-to-peer δίκτυα, η επαλήθευση δεδομένων αποτελεί μια αρκετά σημαντική διαδικασία. Αυτό επειδή τα δεδομένα βρίσκονται διαμοιρασμένα σε πολλά σημεία επιφέρει μια δυσκολία. Στην περίπτωση που γίνει αλλαγή σε ένα σημείο δεδομένων του δικτύου, θα πρέπει στην συνέχεια να ενημερωθούν και όλοι οι επιπλέον συμμετέχοντες του δικτύου. Αν και η διαδικασία του ελέγχου είναι εξαιρετικά σημαντική, είναι χρονοβόρα. Για αυτό τον λόγο, με την χρήση των δένδρων Merkle περιορίζεται ο όγκος των δεδομένων που αποστέλλονται μέσω ενός δικτύου για έλεγχο στο ελάχιστο. Έτσι, αντί να στείλουμε ένα ολόκληρο σύνολο αρχείων μέσω του δικτύου, στέλνουμε απλά ένα κατακερματισμένο αρχείο για να γίνει έλεγχος της εγκυρότητας στο δένδρο. Το πρωτόκολλο λειτουργεί μεταξύ δύο υπολογιστών - χρηστών με τα βήματα:

1. Ο Α στέλνει στον Β το αρχείο για έλεγχο, κατακερματισμένο.
2. Ο Β ελέγχει εάν αυτός ο κατακερματισμός συνάδει με την ρίζα του δένδρου.
3. Εάν υπάρχει συμφωνία η διαδικασία τελειώνει. Σε περίπτωση διαφωνίας μεταξύ των δύο η διαδικασία συνεχίζεται στα παρακάτω.
4. Εάν υπάρχει διαφορά σε ένα μόνο κατακερματισμό, ο Β ζητάει τις ρίζες των δύο υποδέντρων του αρχείου.
5. Ο Α πραγματοποιεί τους ζητούμενους υπολογισμούς του βήματος 4 και τους επιστρέφει στον Β.
6. Τα βήματα 4 και 5 επαναλαμβάνονται συνεχώς μέχρι να βρεθεί το/τα δεδομένο(α) που δεν συνάδουν με την ορθότητα του δικτύου.

Στην περίπτωση του Blockchain, τα δένδρα Merkle θεωρούνται ιδιαίτερα σημαντικά καθώς κάνουν δυνατή την επαλήθευση μίας συναλλαγής χωρίς να χρειάζεται να πραγματοποιηθεί λήψη ολόκληρων των δεδομένων του δικτύου. Ο λόγος που η διαδικασία είναι σημαντική αφορά την ταχύτητα. Καθώς τα συνολικά δεδομένα ενός δικτύου μπορεί να είναι ιδιαίτερα μεγάλα σε όγκο, μπορεί να πραγματοποιηθεί η επιβεβαίωση τα συναλλαγής σε ελάχιστο χρόνο, χωρίς ανάγκη αναμονής για λήψη επιπρόσθετων δεδομένων.

Η λειτουργεία που επιτελούν τα δένδρα merkle είναι ο έλεγχος της εγκυρότητας – αυθεντικότητας των δεδομένων που διακινούνται εντός ενός Blockchain. Η διαδικασία του ελέγχου εγκυρότητας μπορεί να πραγματοποιηθεί για να ελεγχθεί η ορθότητα των δεδομένων που περιέχει το εκάστοτε block με τη διαδικασία κατακερματισμού. Με τον κατακερματισμό από τα φύλλα - κόμβους πρέπει στο τέλος να συμφωνεί με τις κατακερματισμένες τιμές γονικών κόμβων που εμφανίζονται στη ρίζα. Με το πέρας αυτής της διαδικασίας και εφόσον δεν προκύψουν προβλήματα και απορρίψουν κάποιο κόμβο, αποδεικνύεται ότι ένα φύλλο αποτελεί κομμάτι του δένδρου.

(Brilliant, 2020)

(Πολυτίδου, 2018)

2.1.14 Αλυσίδα

Ο όρος αλυσίδα αναφέρεται στον τρόπο που θεωρητικά είναι συνδεμένα μεταξύ τους τα block του δικτυού, εφόσον το ένα συνδέεται με το αμέσως προηγούμενο - επόμενο μέσω δεδομένων είναι

σαν να αποτελούν μια αλυσίδα, όπου οι κρίκοι συνδέονται μεταξύ τους. Ο τρόπος που τα block συνδέονται μεταξύ τους αφορά τα δεδομένα που παρουσιάζονται στην κεφαλή του καθενός. Ειδικότερα στην κεφαλή υπάρχει το parent block hash που συνδέει το παρόν block ν με το αμέσως προηγούμενο block ν-1. Αυτή η τιμή προκύπτει μέσω της διαδικασίας κατακερματισμού σε συγκεκριμένα δεδομένα της κεφάλης και με τη χρήση των κρυπτογραφικών αλγορίθμων που προαναφέρθηκαν για την προστασία δεδομένων του δικτύου.

2.1.15 Τροποποίηση της αλυσίδας (Forking)

Η διαδικασία πραγματοποίησης αλλαγών και εφαρμογής αυτών με διαδικασία αποστολής ενημερώσεων είναι μια όχι και τόσο εύκολη διαδικασία. Η συγκεκριμένη διαδικασία στον τεχνολογικό κόσμο είναι γνωστή ως *forking*. Το επίπεδο δυσκολίας διαφέρει. Στα δίκτυα που λειτουργούν με άδεια και υπάρχουν συγκεκριμένοι χρήστες, συστήματα, αλγόριθμοι και πρωτόκολλα, η διαδικασία μπορεί να πραγματοποιηθεί με σχετική ευκολία και ταχύτητα. Ωστόσο στα δίκτυα Blockchain που λειτουργούν χωρίς την ανάγκη απόκτησης άδειας η διαδικασία είναι ιδιαίτερα δύσκολη καθώς οι τιμές των αντίστοιχων χαρακτηριστικών που αναφέρθηκαν στα δίκτυα με άδεια είναι πολύ μεγαλύτερες σε όγκο. Τα *forks* που μπορούν να εκτελεστούν είναι δύο ειδών, τα *soft forks* και τα *hard forks* ανάλογα με το είδος της αλλαγής που πρόκειται να φέρουν στο δίκτυο. Τα forks πραγματοποιούνται για την διόρθωση σφαλμάτων, την προσθήκη νέων χαρακτηριστικών στο σύστημα ή ακόμη για την γρήγορη διακοπή κυβερνοεπιθέσεων που πραγματοποιούνται.

Soft Forks, είναι η διαδικασία που παρέχει αλλαγές σε μια εφαρμογή που είναι συμβατή και με προγενέστερες εκδόσεις της εφαρμογής (*backwards compatible*). Συνήθως πρόκειται για μια απλή αλλά ουσιαστική διόρθωση ενός σφάλματος μιας εφαρμογής. Μετά τη διαδικασία, εάν κάποιοι κόμβοι δεν έχουν πραγματοποιήσει την αναβάθμιση, θα μπορούν να επικοινωνούν με το δίκτυο και να πραγματοποιούν συναλλαγές με τους ενημερωμένους κόμβους. Στην περίπτωση που κανένας ή ένα μικρό ποσοστό των κόμβων πραγματοποιήσει την αναβάθμιση, το δίκτυο δεν θα λειτουργεί με τους νέους κανόνες αλλά με τους παλιούς που υπερισχύουν στο δίκτυό.

Hard Forks, πρόκειται για μια τελείως διαφορετική διαδικασία. Αρχικά η ενημέρωση δεν είναι συμβατή και με προγενέστερες εκδόσεις τις εφαρμογής (*non-backwards compatible*). Το hard fork προγραμματίζεται πότε πρόκειται να συμβεί, είτε μία συγκεκριμένη χρονική στιγμή ή πιο συχνά μετά τη δημιουργία ενός προκαθορισμένου block. Πλέον στο Blockchain έρχονται ριζικές αλλαγές στον πυρήνα της εφαρμογής και προκαλείται διάσπαση της αλυσίδας που υπήρχε έως εκείνη τη χρονική στιγμή. Στη συνέχεια δημιουργείται ακόμη μια καινούρια αλυσίδα από την οποία θα συνεχίσει επιπλέον τη λειτουργία του το δίκτυο. Αξίζει να σημειωθεί ότι και η παλαιά αλυσίδα θα συνεχίσει να υφίσταται, αλλά πλέον στην παλαιά αλυσίδα δεν επιτρέπεται η πραγματοποίηση επιπλέον αλλαγών. Υπάρχει το περιθώριο ελευθερίας και όποιος δεν πραγματοποιήσει την ενημέρωση θα μπορεί, εάν θέλει, να συνεχίσει τη συμμετοχή του στην παλαιά αλυσίδα. Στην παλαιά αλυσίδα οι αλλαγές θα γίνονται αποδεκτές μόνο από κόμβους που τρέχουν την παλαιά έκδοση.

Παράδειγμα εφαρμογής ενός hard fork αποτελεί το παρακάτω: το 2016, όταν και στο δίκτυο Ethereum δημιουργήθηκε ένα έξυπνο συμβόλαιο με όνομα *Αποκεντρωμένος Αυτόνομος Οργανισμός* (*Decentralized Autonomous Organization – DAO*) στο οποίο μέσω ιδιωτικών κεφαλαίων είχαν επενδυθεί περίπου $150 εκατομμύρια. Λόγω κενών ασφάλειας που υπήρχαν στη λειτουργεία των έξυπνων συμβολαίων, μια ομάδα κατάφερε και εξόρυξε από το δίκτυο περίπου $50 εκατομμύρια στην τότε αντιστοιχία που υπήρχε για το Ether, το κρυπτονόμισμα του Ethereum. Για την καταπολέμηση αυτής της επίθεσης προτάθηκε να πραγματοποιηθεί ένα hard fork και να σπάσει η αλυσίδα. Η καινούρια αλυσίδα συνέχισε κανονικά τη λειτουργεία του Ethereum, ενώ διατηρήθηκε και η παλιά, η οποία έλαβε το όνομα *Ethereum Classic*. Στην καινούρια πλέον δεν υπήρχε το κενό ασφαλείας και τα χρήματα κατάφεραν να επιστρέψουν στους αρχικούς κατόχους, χάρις την βοήθεια των δημιουργών του Ethereum.

(Binance.academy, χ.χ.)

(Nodes, n.d.)

2.2 Λόγοι χρήσης και μη των Blockchain

Τα βασικά πλεονεκτήματα της χρήστης τεχνολογίας Blockchain είναι:

- **Πλήρης ιστορικότητα**, οι τυπικές βάσεις δεδομένων για κάθε ερώτημα που εκτελούμε σε αυτές μας επιστρέφουν ένα στιγμιότυπο με τα δεδομένα που υπάρχουν στη βάση εκείνη τη συγκεκριμένη στιγμή. Το Blockchain ουσιαστικά είναι μια βάση δεδομένων με ιστορικότητα η οποία διαθέτει το πλήρες ιστορικό και όλες τις τιμές που υπήρχαν από την πρώτη στιγμή λειτουργείας του δικτύου.
- **Δυσκολία στις κυβερνοεπιθέσεις**, καθώς το σύστημα είναι διαμοιρασμένο σε πολλούς υπολογιστές, δεν υπάρχει κάποια κεντρική βάση δεδομένων την οποία hacker θα μπορούσαν να χρησιμοποιήσουν για την εκτέλεση κακόβουλων επιθέσεων.
- **Μη ύπαρξη κεντρικής αρχής**, εφόσον πρόκειται για πλήρως διαμοιρασμένο σύστημα σε πολλά σημεία, δεν υπάρχει η ανάγκη ύπαρξης μιας κεντρικής αρχής για την ορθή λειτουργεία του. Με αυτόν τον τρόπο καταφέρνει να μειώνει κατά πολύ τα λειτουργικά έξοδα σε όποιον το διαχειρίζεται.

Ωστόσο δεν πρόκειται για ένα τέλειο σύστημα το οποίο έχει έρθει για να προσφέρει λύσεις παντού. Υπάρχουν τομείς που τη συγκεκριμένη χρονική στιγμή δεν μπορεί να προσφέρει τη βέλτιστη δυνατή λύση σε σύγκριση με κλασσικές υπολογιστικές εφαρμογές.

Αν και δημιουργεί αξιοπρεπείς λύσεις στον χρηματοοικονομικό τομέα κατά κύριο λόγο δεν αποτελεί τη βέλτιστη λύση, καθώς ο τραπεζικός τομέας χρειάζεται ένα σύστημα που θα εκτελεί τεράστιο όγκο συναλλαγών ανά κλάσματα δευτερολέπτου. Το Blockchain θα χρειάζεται τεράστια υπολογιστική και ενεργειακή ισχύ για να λειτουργεί άρτια σε τέτοιες συνθήκες. Ωστόσο δημιουργούνται συνεχώς νέα πρωτόκολλα συναίνεσης τα οποία μειώνουν κατά πολύ την ανάγκη ισχύος.

Λόγω της φύσης του, το Blockchain παρέχει διαφάνεια πάντοτε. Για το συγκεκριμένο λόγο μέχρι στιγμής δεν αποτελεί τη βέλτιστη λύση για την διαχείριση και διαφύλαξη απόρρητων πληροφοριών και εγγράφων. Ωστόσο, το παραπάνω πρόβλημα μπορεί να επιλυθεί με την σωστή επιλογή τύπου Blockchain και αλγορίθμων συναίνεσης που το τροποποιούν σε ένα άκρως ιδιωτικό δίκτυο.

2.3 Πρωτόκολλα συναίνεσης

Ένα σημαντικό χαρακτηριστικό για τη δημιουργία ενός Blockchain είναι ο καθορισμός των δυνατοτήτων δημιουργίας καινούριων block. Σε αυτό το πρόβλημα δίνεται λύση με την επιλογή πρωτοκόλλων συναίνεσης. Η επιλογή τέτοιου πρωτοκόλλου είναι καθοριστικής σημασίας, καθώς περιορίζει τις πλατφόρμες που θα επιλεχθούν στη συνέχεια όπως και τις δυνατότητες που θα μπορεί να έχει το Blockchain. Αλλά τί πραγματικά είναι τα πρωτοκολλά συναίνεσης;

Ο όρος συναίνεση (*consensus*) αναφέρεται στη συμφωνία που θα πρέπει να υπάρχει μεταξύ των κόμβων για την κατάσταση του Blockchain. Ένα γνωστό πρόβλημα που μπορεί να μας κάνει κατανοητό τον παραπάνω ορισμό, είναι το πρόβλημα των βυζαντινών στρατηγών (*Byzantine Generals Problem*). Το πρόβλημα αυτό περιγράφει μία κατάσταση όπου οι στρατηγοί έχουν φτάσει έξω από μία πόλη και είναι στα πρόθυρα να την πολιορκήσουν. Ένα μέρος των στρατηγών προτείνει επίθεση, ενώ το υπόλοιπο υποχώρηση. Χωρίς τη κοινή απόφαση για επίθεση η ήττα είναι αναπόφευκτη. Έτσι και στα Blockchain που και βασική ιδέα είναι η μη ύπαρξη κάποιας κεντρικής αρχής για τη λήψη αποφάσεων, πρέπει να υπάρχει ένας τρόπος που θα χρησιμοποιείται για τη επιλογή απόφασης δημιουργίας νέων block. Μέχρι στιγμής υπάρχουν αρκετά πρωτόκολλα συναίνεσης, ωστόσο νέα δημιουργούνται συχνά καθώς το Blockchain αναπτύσσεται όλο και σε περισσοτέρους τομείς.

Όταν ένας χρήστης εισέρχεται σε ένα Blockchain δίκτυο, αποδέχεται την αρχική κατάσταση του δικτύου η οποία είναι δημοσιευμένη στο genesis block που έχει δημοσιευτεί από τους δημιουργούς πριν το δίκτυο καν γίνει διαθέσιμο σε περεταίρω χρήστες. Κάθε block που δημιουργείτε έπειτα από το αρχικό, οι κανόνες που θα ακολουθήσει καθορίζονται από το πρωτόκολλο συναίνεσης που έχει επιλεχθεί. Ασχέτως του τρόπου λειτουργείας που καθορίζει το πρωτόκολλο, για να γίνει η προσθήκη ενός block όπως και με το πρόβλημα των βυζαντινών στρατηγών, πρέπει να υπάρξει ομόφωνη απόφαση που θα επικυρώνει την εγκυρότητα του block ώστε να προστεθεί στην αλυσίδα.

Επιπλέον μια πληθώρα ιδιοτήτων και διαδικασιών που υπάρχουν στο παρασκήνιο για το πώς λειτουργούν τα πρωτόκολλα συναίνεσης, ωστόσο ο απλός χρήστης δεν χρειάζεται να τα ξέρει καθώς αυτά εξ ολοκλήρου διαχειρίζονται αυτόματα από κάποιο λογισμικό σύστημα.

Τα πρωτόκολλα συναίνεσης μπορούν να κατηγοριοποιηθούν σε τρείς επιμέρους κατηγορίες.

1. Βασισμένα σε πρωτόκολλα *PoW,* όπου είναι απαραίτητα η παραγωγή κάποιου έργου
2. Πιο αποτελεσματικά και με χαμηλότερη κατανάλωση ενέργειας πρωτόκολλα (*Proof-of-X*) που η λογική τους βασίζεται στα PoW.

3. Υβριδικά πρωτόκολλα, τα οποία αποτελούν παραλλαγές των κλασσικών πρωτοκόλλων και λειτουργούν με την ύπαρξη επιτροπών

Στις ακόλουθες υπό-ενότητες, αναλύονται θεωρητικά οι παραπάνω τρείς κατηγορίες καθώς και διάφορα από τα δημοφιλή πρωτόκολλα συναίνεσης. Παράλληλα παρουσιάζεται και ο τρόπος λειτουργείας τους και παραδείγματα χρήσης αυτών.

2.3.1 Proof-of-Work (PoW)

Στο μοντέλο Proof-of-Work (PoW), το οποίο πρωτοεμφανίστηκε μαζί με τα Bitcoin, ένας χρήστης δημιουργεί το επόμενο δυνατό block στην αλυσίδα με το να καταφέρει να είναι ο πρώτος που θα βρει και θα δώσει τη λύση σε έναν δύσκολο και απαιτητικό υπολογισμό. Ο τρόπος που δημιουργούνται τέτοια προβλήματα είναι, κάνοντας τα δύσκολα στον υπολογισμό αλλά εύκολα στην επαλήθευση της λύσης. Ό μόνος τρόπος για την επίλυση του προβλήματος, είναι η πραγματοποίηση επαναλαμβανόμενων δοκιμών μέσω αλγορίθμων. Οι κόμβοι λαμβάνουν από την κεφαλή του επόμενου block κατακερματισμένες τιμές της τιμής nonce. Το ζητούμενο σε ένα τέτοιο πρόβλημα είναι, η τιμή κατακερματισμού που υπάρχει στην κεφαλή ενός block να είναι μικρότερη ή ίση από την τιμή που ορίζεται ως δυσκολία του block. Η δυσκολία του προβλήματος συνεχώς αυξάνεται καθώς όλο και περισσότεροι άνθρωποι και γρηγορότεροι υπολογιστές, λαμβάνουν μέρος στην διαδικασία της επίλυση μιας και η συγκεκριμένη διαδικασία επιβραβεύει τους χρήστες με ένα πόσο σε κρυπτονομίσματα.

Το πρωτόκολλο PoW απαιτεί απ' όλους τους κόμβους να ελέγξουν τη λύση και σε περίπτωση ομοφωνίας να την δεχθούν. Σε αντίθετη περίπτωση, η λύση απορρίπτεται και το block δεν δημιουργείται. Μιας και συμμετέχουν πολλοί σε τέτοια δίκτυα υπάρχει μια μικρή πιθανότητα να προκύψει παρόμοια λύση παραπάνω από μία φορά ταυτόχρονα. Σε αυτή την περίπτωση, δημιουργούνται διακλαδώσεις στην αλυσίδα και σπάει σε επιμέρους κομμάτια, από την οποία συνεχίζει κανονικά η εξέλιξή της. Η χρήση του συγκεκριμένου πρωτοκόλλου, βοηθά στην καταπολέμηση του φαινομένου της σιβυλλικής επίθεσης , ενός φαινομένου κυβερνοεπίθεσης που αναλύεται στην συνέχεια.

Το ποιο γνωστό παράδειγμα χρήσης του PoW, είναι το Bitcoin. Στη συγκεκριμένη πλατφόρμα, η δυσκολία των προβλημάτων μεταβάλλεται με βάση πόσοι χρήστες εργάζονται για την επίλυση του προβλήματος παράλληλα, καθώς και με την ολική υπολογιστική ισχύ που έχει το δίκτυο ανά πάσα στιγμή. Κατά μέσο όρο η δημιουργία ενός block στο Bitcoin διαρκεί 10 λεπτά.

(Yaga & al., 2018)

2.3.2 Proof-of-Stake (PoS)

Το μοντέλο Proof-of-Stake (PoS) έχει βασιστεί στην ιδέα ότι όσο περισσότερο ένας χρήστης έχει

επενδύσει στο δίκτυο τόσο περισσότερο θα ελπίζει στην θετική και όχι στην αρνητική του εξέλιξη. Ο όρος της συνεισφοράς (stake) αναφέρεται στο σύνολο της ολικής επένδυσης που έχει κάνει κάποιος στο δίκτυο. Ειδικότερα, στα συγκεκριμένα δίκτυα η επένδυση σχετίζεται με τον αριθμό κρυπτονομισμάτων που ο χρήστης έχει επενδύσει στο σύστημα, με οποιοδήποτε τρόπο (είτε μέσω της κατοχής τους, είτε μέσω του συνόλου που έχει διακινήσει σε ένα συγκεκριμένο δίκτυο) και όχι με το σύνολο των υπολογιστικών πόρων που συνεισφέρει στο δίκτυο. Για τη λειτουργεία δικτύων που βασίζονται στο PoS, δεν υπάρχει η διαδικασία όπως στα PoW, όπου οι χρήστες εκτελούν δύσκολους υπολογισμούς – επομένως η χρήση μεγάλης ισχύος δεν έχει καμία διαφορά για τους συμμετέχοντες.

Υπάρχουν τέσσερεις μέθοδοι, οι οποίοι παρουσιάζονται παρακάτω, πάνω στους οποίους το PoS αναγνωρίζει και διαχειρίζεται τη συνεισφορά (stake) του κάθε χρήστη, ώστε να επιλέξει έναν χρήστη για την έκδοση ενός block. Ανεξαρτήτως με το ποια μέθοδος επιλέγεται, ο χρήστης με τη μεγαλύτερη συνεισφορά έχει πάντα και τη μεγαλύτερη πιθανότητά δημοσίευσης του επόμενου block.

1. **Η τυχαία επιλογή** χρηστών που έχουν συνεισφέρει στο δίκτυο, κατά τη συγκεκριμένη μέθοδο, το δίκτυο κοιτάει τις συνεισφορές των χρηστών. Οι χρήστες με το μεγαλύτερο σύνολο προσφοράς έχουν και την ανάλογη, ισόποση με την συνεισφορά τους σε ποσοστό ευκαιρία να επιλεχθούν για τη δημιουργία επόμενων block.
2. **Πολλαπλή ψηφοφορία**, κατά τη συγκεκριμένη κατάσταση το σύστημα παρέχει ελευθερία και δημοκρατία. Αυτοβούλως το σύστημα με αλγορίθμους που έχουν καθοριστεί, πρόκειται να επιλέξει μερικούς από τους χρήστες για τη δημιουργία του επόμενου block. Στη συνέχεια όλοι οι επιλεχθέντες χρήστες πρόκειται να εκτελέσουν ψηφοφορία, ώστε να επιλεχθεί ο χρήστης που θα το εκδώσει. Η ψηφοφορία ενδέχεται να διεξαχθεί για αρκετές φορές, έως να υπάρξει ομόφωνη απόφαση από όλους.
3. **Συστήματα ανάθεσης**, κατά τη συγκεκριμένη μέθοδο οι χρήστες ψηφίζουν κόμβους να γίνουν κόμβοι δημιουργίας (publishing nodes), ώστε να τους αναθέτουν εργασίες και οι κόμβοι να δημοσιεύουν τα block αντί των χρηστών. Κατά τη συγκεκριμένη ψηφοφορία, η επιρροή του κάθε χρήστη στην τελική απόφαση, διαμορφώνεται ανάλογα με την συνολική συνεισφορά που έχει προσφέρει στο δίκτυο. Οι κόμβοι που κερδίζουν στην ψηφοφορία, αναλαμβάνουν τη δουλειά για την επικύρωση και τη δημιουργία νέων block. Στη συγκεκριμένη κατηγορία οι κόμβοι δημιουργίας έχουν μεγάλο ανταγωνισμό από άλλους κόμβους που θέλουν να γίνουν και αυτοί δημιουργοί και για αυτό το λόγο η διαδικασία την ψηφοφορίας διεξάγεται συνεχώς
4. **Συστήματα coin aging**, κατά τη συγκεκριμένη μέθοδο, διαχωρίζονται οι χρήστες που απλά κατέχουν νομίσματα για αρκετό καιρό από αυτούς που τα απέκτησαν πρόσφατα. Μέσο του αλγορίθμου, η ηλικία των νομισμάτων χρησιμοποιείται για τον υπολογισμό της συνεισφοράς (weight stake) και της ανταμοιβή συνεισφοράς (staking reward).

Ένα παράδειγμα χρήσης του πρωτοκόλλου PoS είναι τα κρυπτονομίσματα Cosmos (ATOM) και Tezos (XZT) τα οποία προσφέρουν πολύ καλό ετήσιο επιτόκιο σε σχέση με τον ανταγωνισμό. Πολλοί από τους χρήστες κρυπτονομισμάτων PoS, κάνουν επενδύσεις σε αυτά και για την μακροχρόνια απόκτηση παθητικού εισοδήματος.

(Yaga & al., 2018)

(Μπεκρή, 2020)

2.3.3 Υβριδικοί αλγόριθμοι συναίνεσης

Τα υβριδικά μοντέλα αλγορίθμων συναίνεσης αποτελούν την τεχνική της δημιουργίας εναλλακτικής μορφής αλγορίθμων, βασισμένα πάντα στους κλασσικούς και ευρέως διαδεδομένους μηχανισμούς συναίνεσης PoW ή PoX. Στη συγκεκριμένη περίπτωση, η απόφαση για τη δημιουργία των νέων block δεν παίρνεται ατομικά από ένα κόμβο. Η απόφαση λαμβάνεται από ένα σύνολο κόμβων οι οποίοι με τη σειρά τους αποτελούν μία ή αρκετές επιτροπές (committees). Η διαδικασία μπορεί να πραγματοποιηθεί πχ. με διαδικασίες ψηφοφορίας που παρουσιάζονται στα ανάλογα μοντέλα. Με αυτή την τεχνική, παρακάμπτονται τα αρνητικά στοιχεία που υπήρχαν σε άλλους αλγορίθμους που λειτουργούν ατομικά βάση κάποιας ισχύος ή συνολικών συνεισφορών, όπως ολική αδυναμία συνέπειας και χαμηλή ανεκτικότητα σε σφάλματα.

Αξίζει να σημειωθεί ότι η τεχνική ύπαρξης της επιτροπής αποτρέπει πιθανές σιβυλλικές επιθέσεις στο δίκτυο, ένας τρόπος επίθεσης που αναλύεται στη συνέχεια της εργασίας. Σε αυτή την κατηγορία συστημάτων μπορούν να διακριθούν δύο επιμέρους είδη, σε αυτά που η απόφαση λαμβάνεται από μια επιτροπή και σε αυτά που λαμβάνεται από περισσότερες.

Αρχικά με την περίπτωση αλγορίθμων συναίνεσης όπου η απόφαση παίρνεται από μια μόνο επιτροπή, σε κάθε μια επιτροπή, εισάγονται κόμβοι που θα χρησιμοποιηθούν για τη διαδικασία της ψηφοφορίας βάση συγκεκριμένων κριτηρίων. Οι επιτροπές κατηγοριοποιούνται με βάση τον τύπο του δικτύου. Στα δίκτυα που χρειάζεται άδεια για συμμετοχή, οι επιλεχθέντες για την επιτροπή είναι σχετικά οι ίδιοι χρήστες για αρκετό καιρό λόγω της εμπιστοσύνης που υπάρχει. Από την άλλη όμως στα δίκτυα που λειτουργούν και δεν χρειάζεται άδεια για συμμετοχή, οι επιλεχθέντες για την επιτροπή μπορούν να είναι στατικές ή δυναμικές οντότητες και η θέση τους στην επιτροπή μπορεί να μεταβληθεί.

Στην περίπτωση των αλγορίθμων συναίνεσης, όπου η απόφαση παίρνεται από πολλαπλές επιτροπές, η γενικότερη κατάσταση διαφέρει. Η βασικότερη ιδέα για την ύπαρξη πολλών επιτροπών είναι η επίλυση προβλημάτων επεκτασιμότητας, ώστε να μπορούν οι κόμβοι να αποφασίζουν για αρκετά μεγαλύτερο όγκο αποφάσεων. Οι επιτροπές κατηγοριοποιούνται βάση της τοπολογίας τους. Υπάρχουν οι επίπεδες τοπολογίες και οι τοπολογίες ιεραρχίες. Η βασική λειτουργεία και των δύο τοπολογιών είναι παρόμοια, η λήψη αποφάσεων. Ωστόσο στις ιεραρχικές, η ιδιότητα λήψης αποφάσεων μετατίθεται στους ανώτερους, όπως γίνεται και σε ένα κλασσικό επιχειρηματικό περιβάλλον.

Παράδειγμα χρήσης των υβριδικών πρωτοκόλλων, μεταξύ πολλών, αποτελεί το μοντέλο του Delegated-Proof-of-Stake και το Proof-of-Authority/Proof-of-Identity. Επιπλέον παράδειγμα αποτελεί και η πλατφόρμα ανάπτυξης εφαρμογών Quorum. Όλα τα παραπάνω, αναλύονται στην συνέχεια.

(Kouklas, 2018)

(Μπεκρή, 2020)

2.3.4 Proof-of-Elapsed-Time (PoET)

Στο μοντέλο Proof-of-Elapsed Time (PoET), κάθε κόμβος που δημιουργεί block, ζητάει έναν χρόνο αναμονής από ένα ασφαλές σύστημα διαχείρισης χρόνου που υπάρχει στον υπολογιστή του. Το ασφαλές αυτό σύστημα λαμβάνει τον κώδικα PoET και πρόκειται να δημιουργήσει έναν τυχαίο χρόνο αναμονής τον οποίο θα τον επιστρέψει στο λογισμικό του ενεργού κόμβου που δημοσιεύει στο δίκτυο κάνοντας χρήση της τεχνολογίας Software Guard Extensions (SGX), τεχνολογία που η Intel, κατασκευαστής επεξεργαστών, βάζει στα chip της. Οι κόμβοι με τη σειρά τους λαμβάνουν αυτόν τον χρόνο και παραμένουν ανενεργοί για αυτό το διάστημα που έχει προκαθοριστεί. Με το τέλος αυτής της χρονικής περιόδου ο κόμβος αλλάζει κατάσταση από ανενεργός σε ενεργός και δημιουργεί το block, ενώ παράλληλα πραγματοποιείται μια διαδικασία κατά την οποία, ταυτόχρονα όλοι οι κόμβοι που βρίσκονται στην κατάσταση αδράνειας ενημερώνονται ότι το block δημιουργήθηκε και αλλάζουν κατάσταση σε ενεργή. Στη συνέχεια πραγματοποιείται πάλι η διαδικασία που προαναφέρθηκε με μία κυκλική ροή.

Στην συγκεκριμένη περίπτωση υπάρχει και μια πιθανή περίπτωση κατάχρησης του τρόπου λειτουργείας του δικτύου. Ωστόσο για την αποφυγή τέτοιων περιπτώσεων, ο χρόνος ελέγχεται αυτόματα από το λογισμικό που υπάρχει σε επεξεργαστές. Για την άρτια και δίκαιη λειτουργεία, ο χρόνος αναμονής θα πρέπει να επιλέγεται εντελώς τυχαία και να μην προεπιλέγεται από χρήστες, οι οποίοι θα τον γνωρίζουν, με στόχο την πραγματοποίηση μιας κακόβουλης ενέργειας. Επιπλέον θα πρέπει να ελέγχεται και η χρονική στιγμή που ο κόμβος μετέβη σε κατάσταση αναμονής, δηλαδή ότι δεν ξεκίνησε τη διαδικασία αναμονής προγενέστερα από άλλους κόμβους, προκειμένου να κερδίσει στη διαδικασία της δημιουργίας.

Παράδειγμα χρήσης του PoET αποτελούν συστήματα βασισμένα στην πλατφόρμα Hyperledger Sawtooth, που δίνει τη δυνατότητα χρήσης του μοντέλου.

(Frankenfeld, 2020)

2.3.5 Proof-of-Burn (PoB)

Το μοντέλο *Proof-of-Burn (PoB)*, αποτελεί ένα διαφορετικό και καινοτόμο αλγόριθμο που έχει ως βασικό στόχο την επίλυση των προβλημάτων υψηλής ζήτησης ενέργειας και υπολογιστικής ισχύος που χρειάζεται το μοντέλο PoW κατά τη λειτουργεία του. Από τους πιο βασικούς λόγους που δημιουργήθηκε το πρωτόκολλο ήταν για την καταπολέμηση του φαινομένου της διπλής σπατάλης.

Η βασική αρχή λειτουργίας του συστήματος είναι ότι οι χρήστες “καίνε” ένα σύνολο νομισμάτων, στέλνοντας τα σε μια διεύθυνση που κανένας δεν έχει έλεγχο και αυτά μετατρέπονται σε μη διαθέσιμα για σπατάλη νομίσματα. Αυτή η διαδικασία δεν σπαταλά ποσά ενέργειας και

διασφαλίζει ότι το δίκτυο θα είναι συνεχώς ενεργό. Τα νομίσματα που αποστάλθηκαν από χρήστες, παρέχουν δικαιώματα στους ίδιους να δημιουργήσουν αριθμό block στην αλυσίδα, αναλογικά με το ποσό τον νομισμάτων που έστειλαν για "κάψιμο". Ανάλογα με την υλοποίηση που ακολουθεί κάθε δίκτυο, δίνονται δυνατότητες αποστολής για "κάψιμο" νομισμάτων, είτε από κάποιο τρίτο κρυπτονόμισμα (πχ. Bitcoin, Ethereum) είτε κρυπτονομίσματα που διαχειρίζεται το εκάστοτε Blockchain.

Αξίζει να σημειωθεί ότι η υλοποίηση του PoB, αποτελεί ένα πρωτόκολλο που συνοδεύεται από υψηλό ρίσκο, καθώς δεν υπάρχει εγγύηση για το εάν ο χρήστης που στέλνει για "κάψιμο" ένα x ποσό νομισμάτων, θα το λάβει πίσω τουλάχιστον ισόποσα.

Παράδειγμα χρήσης του PoB, αποτελεί το κρυπτονόμισμα Slimcoin(SLM), το οποίο κάνει χρήση ενός συνόλου αλγορίθμων, του PoW, PoS και του PoB. Κατά τη λειτουργεία του PoB, επιτρέπεται στους miners να κάψουν το ποσό κρυπτονομισμάτων που επιθυμούν και ως αντίτιμο οι ίδιοι λαμβάνουν την πιθανότητα προσπάθειας για τη δημιουργία επόμενων block καθώς και την πιθανότητα να λαμβάνουν block για μεγάλο χρονικό διάστημα, το οποίο είναι τουλάχιστον ένα έτος.

(Bano & al., 2017)

2.3.6 Proof-of-Authority (PoA) ή Proof-of-Identity (PoI)

Το μοντέλο Proof-of-Authority (PoA), γνωστό και ως Proof-of-Identity, είναι ένας καινούριος αλγόριθμος συναίνεσης που προσφέρει υψηλή απόδοση και υψηλή ανοχή σε σφάλματα, που μπορεί να εφαρμοστεί σε κάθε τύπο δικτύου Blockchain, αλλά συνήθως συναντάται λόγω της φύσης του σε ιδιωτικά δίκτυα υψηλής εμπιστοσύνης. Η λογική παραμένει ίδια με τους αλγορίθμους PoS και DPoS.

Η βασική ιδέα του PoA είναι ότι δικαιώματα δημιουργίας νέων block παρέχονται στους κόμβους που έχουν λάβει άδεια για τη συγκεκριμένη διαδικασία καθώς και για την ασφάλεια του συστήματος. Για να αποκτηθεί αυτή η δυνατότητα από τους κόμβους, ένας κόμβος θα πρέπει να περάσει από έναν έλεγχο την πρώτη φορά που εισέρχεται στο δίκτυο και θα πρέπει να έχουν αποδεδειγμένες και επαληθεύσιμες ταυτότητες στο δίκτυο. Ο κόμβος ουσιαστικά σε αυτή την περίπτωση "ποντάρει" την φήμη που διαθέτει στο δίκτυο για τη δημοσίευση block. Βασική διαφοροποίηση με τα υπόλοιπα πρότυπα συναίνεσης και γενικά με την ιδέα του Blockchain αποτελεί το ότι υπάρχουν άτομα για την επικύρωση συναλλαγών, αρά το σύστημα γίνεται κεντροποιημένο πλέον.

Στα συγκεκριμένα Blockchain οι χρήστες επηρεάζουν τον τρόπο που λειτουργεί το δίκτυο καθώς μπορούν να κρίνουν θετικά ή αρνητικά την λειτουργεία που εκτελούν οι κόμβοι. Έτσι λοιπόν μεταβάλλεται η φήμη των κόμβων. Όσο μεγαλύτερη θετική άποψη έχουν οι χρήστες για τον κάθε κόμβο, τόσο μεγαλύτερο είναι το ποσοστό της συνολικής φήμης που κατέχει. Το ποσοστό επιλογής κόμβου εξαρτάται άμεσα με τη βαθμολογία που διαθέτει από τις αξιολογήσεις.

(Yaga & al., 2018)

2.3.7 Delegated-Proof-of-Stake (DPOS)

Το μοντέλο Delegated-Proof-of-Stake (DPoS), αποτελεί μια επέκταση του PoS και προσφέρει έναν πιο αποτελεσματικό και δημοκρατικό μηχανισμό. Οι συμμετέχοντες αναθέτουν την παραγωγή νέων block σε τρίτους, οι οποίοι επικυρώνουν τις συναλλαγές. Και στο DPoS έχουμε ένα σύστημα ψηφοφορίας στο οποίο η ισχύς της ψήφου για το τελικό αποτέλεσμα διαμορφώνεται ανάλογα με τα χρήματα που ένας χρήστης έχει στην κατοχή του. Το μοντέλο διαφοροποιείται αλλά σαν γενικός κανόνας ισχύει ότι κάθε εκπρόσωπος που ζητά ψήφους παρουσιάζει και μια πρόταση, ώστε να πείσει τους χρήστες και να λάβει τους ψήφους τους. Ο ανταγωνισμός είναι υψηλός, αλλά πολύ κερδοφόρος.

Ο DPoS βασίζεται άμεσα πάνω στους αντιπροσώπους και στη φήμη που οι ίδιοι διαθέτουν. Υπάρχουν όμως και περιπτώσεις όπου ένας εκλεγμένος εκπρόσωπος μπορεί να λειτουργεί μη αποδοτικά. Στην συγκεκριμένη περίπτωση, ο εκπρόσωπος χάνει την θέση του και άμεσα γίνεται αντικατάστασή του από άλλον. Ο αλγόριθμος DPoS πραγματοποιεί τη διαδικασία δημιουργίας block με υψηλή ταχύτητα ενώ παράλληλα επιτρέπει και την μεγαλύτερη επεξεργασία συναλλαγών ανά δευτερόλεπτο, σε συνολικό όγκο. Κατά τη διάρκεια της ψηφοφορίας, οι κάτοχοι κρυπτονομισμάτων, επιλέγουν τα άτομα που θα επικυρώσουν τα νέα block. Ανάλογα το σύστημα και τον φόρτο εργασίας του δικτύου, η παραγωγή νέων block πραγματοποιείται συνήθως κάθε 1 με 2 δευτερόλεπτα. Οι ανταμοιβές που λαμβάνουν οι εκπρόσωποι που κέρδισαν την ψηφοφορία, μοιράζονται στη συνέχεια στα άτομα τα οποία τους εξέλεξαν.

Το πρωτόκολλο εκτός από την ταχύτητα προσφέρει και έναν χαρακτήρα αρκετά πιο δίκαιο από άλλα συνηθισμένα μοντέλα ψηφοφορίας, καθώς η ανταμοιβή που λαμβάνει ο εκλεγμένος αντιπρόσωπος μοιράζεται στη συνέχεια στους εκλέκτορές του.

(Binance Academy, χ.χ.)

2.3.8 Proof-of-Capacity (PoC)

Το μοντέλο Proof-of-Capacity γνωστό και ως Proof-of-Space (PoS) αποτελεί μια εναλλακτική λύση για δίκτυα Blockchain. Κατηγοριοποιείται στην ομάδα των PoX καθώς πραγματοποιεί επίλυση μαθηματικών εξισώσεων αλλά με διαφορετικό τρόπο. Σε αντίθεση με τα άλλα μοντέλα, εδώ μετράει ο συνολικός αποθηκευτικός χώρος που διαθέτει ο κάθε χρήστης, σε οποιαδήποτε απτή συσκευή που έχει στην κατοχή του ο χρήστης ή ακόμη και σε κάποιο υπολογιστικό νέφος (cloud).

Ειδικότερα, σε τέτοιου είδους δίκτυα υπάρχουν τα μέρη (plots), τα οποία σαν ορισμός αντιστοιχούν στον υπολογισμό και στην αποθήκευση λύσεων σε δικό σου αποθηκευτικό χώρο. Όσα περισσότερα μέρη διαθέτεις στην κατοχή σου, τόσο μεγαλύτερη είναι και η πιθανότητα να κερδίσεις το επόμενο block που θα δημιουργηθεί. Ο συγκεκριμένος τύπος αλγορίθμου είναι αρκετά περίπλοκος κατά τον υπολογισμό του. Οι συμμετέχοντες στη διαδικασία της εξόρυξης, για πιθανούς λόγους κερδοφορίας, βάζουν όσα περισσότερα μέρη μπορούν στους αποθηκευτικούς

τους χώρους, τα οποία αξίζει να σημειωθεί αποθηκεύονται στον χώρο του κάθε miner πριν ακόμη αρχίσει η διαδικασία. Η διαδικασία του PoC επομένως, χωρίζεται σε δύο επιμέρους.

Η πρώτη (plotting) αφορά την διαδικασία της επιλογής μερών για την αποθήκευση των plots. Κατά τη συγκεκριμένη διαδικασία, δημιουργούνται όλοι οι πιθανοί συνδυασμοί της τιμής nonce μέσω συνεχών κατακερματισμών στα δεδομένα, ενώ στη διαδικασία συμπεριλαμβάνεται και το αναγνωριστικό του χρήστη. Κάθε nonce περιέχει 8192 (0-8191) κατακερματισμένα δεδομένα. Στη συνέχεια κάθε nonce δημιουργεί με το αμέσως επόμενό του μια ομάδα (scoop). Πχ η τιμή nonce 0 με την τιμή nonce 1 αποτελούν την τιμή scoop 0 και ούτω καθεξής. Κατά το plotting στον αποθηκευτικό χώρο που έχει ορίσει ο κάθε miner κατεβαίνουν δεδομένα με πολύ αργό ρυθμό, ο οποίος μπορεί να κρατήσει μέχρι και αρκετές εβδομάδες, ανάλογα με τα αρχεία. Ο λόγος που υπάρχει τόσο μεγάλη χρονική καθυστέρηση βασίζεται στο επίπεδο δυσκολίας του αλγορίθμου κατακερματισμού. Ο αλγόριθμος που χρησιμοποιείται στο PoC, είναι ο Shabal, ένας αρκετά δύσκολος κρυπτογραφικός αλγόριθμος κατακερματισμού που ακόμη και για τους πιο γρήγορους σημερινούς υπολογιστές αποτελεί σημαντική πρόκληση.

Στο δεύτερο μέρος, πραγματοποιείται η διαδικασία της εξόρυξης (mining), στην οποία ο miner υπολογίζει μια τιμή (scoop number). Κατά τη συγκεκριμένη λειτουργεία, ο miner πηγαίνει στην τιμή x του nonce 1 που υπολόγισε και χρησιμοποιεί τα δεδομένα που βρήκε σε αυτή τη θέση για τον υπολογισμό μιας τιμής προθεσμίας (deadline value). Η παραπάνω διαδικασία συνεχίζει να επαναλαμβάνει τον υπολογισμό μιας τιμής προθεσμίας για κάθε τιμή nonce που βρίσκεται στον αποθηκευτικό χώρο του miner. Μετά τον υπολογισμό όλων των τιμών προθεσμίας, από τον miner πρόκειται να επιλεχθεί η τιμή με την ελάχιστη προθεσμία.

Αν και γίνεται χρήση αρκετά περίπλοκων συναρτήσεων που χρήζουν υπολογισμό, ο μηχανισμός λειτουργείας του μοντέλου είναι αρκετά αποδοτικός και έχει αρκετά προτερήματα. Σε σχέση με άλλα μοντέλα συναίνεσης διατηρεί καλύτερη ενεργειακή απόδοση. Δεν χρειάζεται πολύπλοκα μηχανήματα για την εκτέλεσή του και είναι αρκετά μικρού κόστους για την υλοποίηση, αφού το βασικό απαραίτητο είναι ο αποθηκευτικός χώρος, που στις μέρες μας είναι πάμφθηνος σε οποιαδήποτε μορφή αγοραστεί. Τα μειονεκτήματα του μοντέλου περιλαμβάνουν το χαμηλό ποσοστό υιοθέτησης και τον αυξημένο κίνδυνο ιών που μπορεί να επηρεάσει την ταχύτητα του δικτύου και τις δραστηριότητες εξόρυξης.

(Andrew, 2020)

2.3.9 Σύγκριση των αλγορίθμων συναίνεσης

Στον *Πίνακα 2* συγκρίνονται όλα τα μοντέλα αλγορίθμων που αναλύθηκαν στα κεφάλαια 2.3.1 έως 2.3.8. Για τη σύγκριση λαμβάνονται υπόψη διάφορα κριτήρια που μπορούν να εφαρμοστούν. Μεταξύ αυτών είναι ο τύπος του Blockchain, η διαχείριση ταυτότητας κόμβου, η δυνατότητα επεκτασιμότητας, η ταχύτητα επιβεβαίωσης συναλλαγών, η απόδοση, η εξοικονόμηση ενέργειας, το κόστος συμμετοχής, η οριστικότητα συναλλαγής, η εχθρική ανοχή καθώς και παραδείγματα χρήσης των συγκεκριμένων αλγορίθμων.

Πίνακας 2. *Σύγκριση αλγορίθμων συναίνεσης*

Κριτήρια	*PoW*	*PoS*	*PoET*	*PoB*	*PoA/PoI*	*DPoS*	*PoC/PoS*
Τύπος Blockchain	Δημόσια	Δημόσια Ιδιωτικά	Δημόσια Ιδιωτικά	Δημόσια	Δημόσια Ιδιωτικά Υβριδικά	Δημόσια Ιδιωτικά	Δημόσια
Διαχείριση ταυτότητας κόμβου	Ανοιχτή	Ανοιχτή	Ανοιχτή	Ανοιχτή	Ανοιχτή	Ανοιχτή	Ανοιχτή
Επεκτασιμότητα δικτύου	Υψηλή	Υψηλή	Υψηλή	Μεσαία	Υψηλή	Μεσαία	Χαμηλή
Ταχύτητα επιβεβαίωσης	>100s	<100s	Σχετικό	-	-	<100s	Άμεση
Απόδοση	Χαμηλή	Υψηλή	Χαμηλή	Μέτρια	Υψηλή	Υψηλή	Υψηλή
Εξοικονόμηση ενεργείας	Όχι	Μερική	Μερική	Μερική	Μερική	Μερική	Μερική
Κόστος συμμετοχής	Υψηλό	Σχετικό	Μέτριο	Σχετικό	Σχετικό	Σχετικό	Ελάχιστο
Οριστικότητα συναλλαγής	Πιθανολογική	Πιθανολογική	Πιθανολογική	Πιθανολογική	-	Πιθανολογική	Πιθανολογική
Εχθρική ανοχή	<25% της υπολογιστικής ισχύος	<51% της ολικής επένδυσης	<25% της υπολογιστικής ισχύος	<51% της ολικής επένδυσης	<51% της ολικής επένδυσης	<51% της ολικής επένδυσης	<25% της υπολογιστικής ισχύος
Παραδείγματα χρήσης	Bitcoin	XZT	Intel	Slimcoin	TomoChain	EOS	Burstcoin

Είναι εμφανές λοιπόν, ότι από τη διαδικασία της σύγκρισης δεν μπορεί να προκύψει ξεκάθαρος νικητής. Κάθε μοντέλο έχει άλλες απαιτήσεις και άλλες εφαρμογές στην διαδικασία λήψης αποφάσεων σε κατανεμημένα συστήματα. Η επιλογή του αλγορίθμου θα πρέπει να γίνεται με σκέψη και λαμβάνοντας υπόψιν την διαδικασία που πρόκειται να επιτελεί το σύστημα στο μέλλον.

2.4 Έξυπνα Συμβόλαια – Smart Contracts

Τα έξυπνα συμβόλαια (smart contracts) χρονολογούνται το 1994 όταν και ο Nick Szabo παρουσίασε ένα ψηφιακό πρωτόκολλο που πρόκειται να πραγματοποιεί και να ελέγχει τους όρους καθώς και την πρόοδο εκτέλεσης μιας σύμβασης. Σύμφωνα με τον δημιουργό, οι βασικοί στόχοι των έξυπνων συμβολαίων είναι η καταγραφή των υποχρεώσεων που υπάρχουν και από τις δύο μεριές (συμβαλλόμενος – αντισυμβαλλόμενος), σε ψηφιακή μορφή.

Τα έξυπνα συμβόλαια επεκτείνουν τις δυνατότητες του Blockchain προς επιμέρους κατευθύνσεις. Με τον όρο έξυπνα συμβόλαια, αναφερόμαστε σε συλλογές δεδομένων που δημιουργούνται με τη χρήση κρυπτογραφημένων συναλλαγών στα δίκτυα Blockchain. Η μόνη διαφορά με τα έως τώρα γνωστά συμβόλαια, είναι η ψηφιακή τους υπόσταση. Μπορούν να πραγματοποιηθούν για την ανταλλαγή χρημάτων και όλων των υλικών ή άυλων αγαθών/υπηρεσιών με εύκολο και διαφανή τρόπο, ενώ ταυτόχρονα μειώνουν το κόστος και την πολυπλοκότητα που θα μπορούσε να έχει ένα συμβατικό συμβόλαιο, καθώς δεν υπάρχει κάποιος τρίτος διαμεσολαβητής.

Από τεχνολογικής άποψης, τα έξυπνα συμβόλαια εκτελούνται από κόμβους που συμμετέχουν σε ένα κοινό δίκτυο.

Τα πλεονεκτήματα των έξυπνων συμβολαίων είναι πάρα πολλά, μερικά από τα οποία είναι:

- **Διαφάνεια**, οι όροι κάθε συμβολαίου είναι προσβάσιμοι και ορατοί από κάθε άτομο που σχετίζεται με το συμβόλαιο, έτσι μετά την υπογραφή δεν υπάρχει περιθώριο αμφισβήτησης.
- **Ακρίβεια**, καθώς βασικό προαπαιτούμενο των έξυπνων συμβολαίων είναι όλοι οι όροι να είναι εκτενώς τεκμηριωμένοι.
- **Ταχύτητα**, καθώς η διαδικασία κινείται γρήγορα μέσω αυτοματοποιημένων αλγορίθμων στο δίκτυο, έχει ως αποτέλεσμα την παράκαμψη πολλών παραδοσιακών επιχειρηματικών διαδικασιών και ταχύτητα για την εκτέλεση του συμβολαίου.
- **Ασφάλεια,** όπως και με το σύνολο του Blockchain, έτσι και εδώ χρησιμοποιούνται υψηλοί κρυπτογραφικοί αλγόριθμοί, κάνοντας και τα συμβόλαια από τα ποιο ασφαλή πράγματα που υπάρχουν στο διαδίκτυο.
- **Αποδοτικότητα**, μιας και πρόκειται για προϊόντα που λειτουργούν με την ακρίβεια που προαναφέρθηκε, κάνουν τις επιχειρήσεις που τα διαχειρίζονται πιο αποδοτικές καθώς μπορούν να εκτελούν περισσότερα συμβόλαια στον ίδιο χρόνο που χρειαζόταν να εκτελέσουν ένα και μόνο παραδοσιακό συμβόλαιο.
- **Οικονομία**, καθώς εξαλείφεται η ανάγκη ύπαρξης κάποιου μεσάζοντος ή η συμβολή κάποιας τρίτης επιχείρησης μειώνονται τα κόστη εκτέλεσης των συμβολαίων.
- **Φιλικά προς το περιβάλλον**, καθώς δεν είναι αναγκαία η ύπαρξη καταγραφής του συμβολαίου σε χαρτί, απαιτείται μόνο η ψηφιακή τους ύπαρξη.

Ωστόσο, όπως με τα περισσότερα τεχνολογικά προϊόντα, έτσι και στα έξυπνα συμβόλαια υπάρχουν πιθανά προβλήματα που σχετίζονται με διάφορα θέματα, όπως νομική υπόσταση, αδυναμία πλήρους προσαρμογής, υψηλή εξάρτηση από άτομα με γνώση προγραμματισμού και πιθανή έκθεση των συμβολαίων σε σφάλματα του συστήματος. Η σύνταξη ασφαλών έξυπνων συμβολαίων μπορεί να είναι εξαιρετικά δύσκολη λόγω διάφορων επιχειρηματικών λογικών, καθώς και περιορισμών της εκάστοτε πλατφόρμας.

Αξίζει να σημειωθεί ότι αναφέρθηκε ένα μέρος των θετικών και αρνητικών επιπτώσεων που έχει η χρήση των έξυπνων συμβολαίων και όχι το σύνολο αυτών. Καθώς πρόκειται για τεχνολογία που βρίσκεται υπό ανάπτυξη, συνεχώς θα επιλύονται τα ήδη υπάρχοντα προβλήματα αλλά ίσως εμφανιστούν και καινούρια τα όποια δεν μπορούν να εντοπισθούν τώρα.

Ωστόσο φαίνεται ότι έχουν έρθει για να μείνουν. Με την εμπιστοσύνη που τους επιδεικνύει ο επιχειρηματικός κόσμος, συνεχώς βλέπουμε την υλοποίησή τους όλο και από μεγαλύτερο εύρος επιχειρήσεων. Πιθανόν στο μέλλον να τις δούμε να αντικαταστούν πλήρως τις παραδοσιακές συμβάσεις.

(Alharby, 2017)

(Yaga & al., 2018)

2.5 Πλατφόρμες ανάπτυξης

Οι πλατφόρμες ανάπτυξης (frameworks) στον χώρο του Blockchain και γενικότερα στον τομέα της ανάπτυξης εφαρμογών μπορούν να οριστούν ως ολοκληρωμένες λύσεις λογισμικού που διευκολύνουν και απλοποιούν την διαδικασία ανάπτυξης.

Οι πλατφόρμες ανάπτυξης περιέχουν διάφορα εργαλεία, έτοιμα κομμάτια κώδικα και βιβλιοθήκες που χρησιμοποιούνται στην ανάπτυξη εφαρμογών. Στην περίπτωση των κατανεμημένων συστημάτων, το δίκτυο αποτελείται από τους κόμβους και το λογισμικό που τους διαχειρίζεται. Το λογισμικό στο όλο σύνολο του δικτύου παρέχει δυνατότητες, οι οποίες ποικίλουν και μπορούν να παραμετροποιηθούν για να εφαρμόζουν στις απατήσεις κάθε συστήματος. Μερικά από τα παραδείγματα δυνατοτήτων αφορούν η ταυτοποίηση χρηστών, οι λεπτομέρειες και διαδικασίες κάθε συναλλαγής, τα πρωτοκόλλα συναίνεσης κ.α. Η κάθε εφαρμογή μπορεί επιμέρους να χωριστεί σε δύο μέρη, το επίπεδο συστήματος και το επίπεδο της εφαρμογής.

Η επιλογή μιας πλατφόρμας ανάπτυξης Blockchain είναι ένα σύνθετο ερώτημα, καθώς δεν υπάρχει πλατφόρμα ανάπτυξης που να μπορεί να καλύψει/παρέχει όλες τις απαιτήσεις/δυνατότητες. Οι κύριες προκλήσεις που δημιουργεί η διαδικασία της επιλογής, αφορούν την υπολογιστική ισχύ, τη αποθήκευση και την επεκτασιμότητα που χρειάζεται να κατέχει το σύστημα. Για την καλύτερη επιλογή πλατφόρμας, θα πρέπει να καταγραφούν και να αναλυθούν σωστά και από έμπειρους ειδικούς όλες οι ανάγκες του προβλήματος που θέλουν να φέρουν εις πέρας με την εφαρμογή της Blockchain υλοποίησης. Όσον αφορά τη φύση της πλατφόρμας, το ερώτημα που θα πρέπει να απαντηθεί αφορά στο αν η πλατφόρμα θα βασίζεται σε κάποιο κρυπτονόμισμα, σε έξυπνα συμβόλαια, σε μεταφορά αρχείων κ.α. ώστε να επιλεχθεί και ο κατάλληλος τύπος καθολικού αρχείου (DLT).

Βασικό όμως ερώτημα αποτελεί και το πρωτόκολλο συναίνεσης που θα επιλεχθεί μιας και είναι καθοριστική η επιλογή του καθώς αλλαγές μοντέλου στο μέλλον δημιουργούν προβλήματα. Εάν χρειαστεί να γίνει αλλαγή πρωτοκόλλου συναίνεσης, μονόδρομο αποτελεί η δημιουργία νέου δικτύου Blockchain. Η συγκεκριμένη διαδικασία επιφέρει επιπλέον μεγάλο κόστος για την ανάπτυξη καθώς και αρκετό χαμένο χρόνο.

2.5.1 Ethereum

Εικόνα 7. Ethereum (χ.χ.). [Το λογότυπο της πλατφόρμας ανάπτυξης Ethereum]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.ethereum.org.

Το Ethereum είναι η πιο δημοφιλής πλατφόρμα ανάπτυξης. Πρόκειται για πλατφόρμα ανοιχτού κώδικα η οποία είναι δημοσιευμένη στο GitHub και αρκετές χιλιάδες προγραμματιστές συνεισφέρουν στην ανάπτυξή της, προσθέτοντας νέες δυνατότητες ή κάνοντας διόρθωση

υπαρχουσών σφαλμάτων. Υποστηρίζει τις πιο βασικές γλώσσες προγραμματισμού και πλατφόρμες ανάπτυξης λογισμικού όπως Java, Python, JavaScript, GO, Rust, .Net και Delphi – ενώ η ομάδα της προσπαθεί συνεχώς για την ενσωμάτωση όλο και περισσοτέρων γλωσσών για να κάνει την πλατφόρμα πρόσβαση σε μεγάλο σύνολο προγραμματιστών. Η κατασκευή του Ethereum έγινε με στόχο την δημιουργία Smart Contracts στα Blockchain. Το Ethereum δημιουργήθηκε βασισμένο σε 4 πυλώνες (έξυπνα συμβόλαια, EVM, DApps και απόδοση).

- Τα έξυπνα συμβόλαια, έχουν αναλυθεί σε προηγούμενο κεφάλαιο.
- Το EVM (*Ethereum Virtual Machine*) είναι μια ιδέα δημιουργίας πλατφόρμας ανάπτυξης η οποία θα μπορεί να χρησιμοποιηθεί εξίσου το ίδιο, σε αρκετές γλώσσες προγραμματισμού, κάνοντας το Ethereum μια φιλική πλατφόρμα.
- Τα DApps, είναι αποκεντρωμένες εφαρμογές που κάνουν χρήση έξυπνων συμβολαίων για μια πληθώρα ατομικών και εταιρικών διαδικασιών.
- Για την καλύτερη του απόδοση, το Ethereum κάνει χρήση διάφορων λογισμικών και τεχνικών. Γίνεται χρήση των δένδρων Merkle για την βελτιστοποίηση της διαδικασίας του κατακερματισμού καθώς και για την πιθανή αύξηση της κλιμάκωσης του δικτύου.

Το πιο σύνηθες πρωτόκολλο συναίνεσης, που χρησιμοποίει το δίκτυο είναι το *Proof-of-Work* και το *Proof-of-Stake*, ανάλογα με την υλοποίηση. Οι χρήστες τους συνεισφέρουν μέσω της επίλυσης μαθηματικών αλγορίθμων και της συνεισφοράς κρυπτονομισμάτων. Το νόμισμα που χρησιμοποιείται είναι το Ethereum (ETH) – το οποίο την παρούσα στιγμή αποτελεί το 2^{ο} μεγαλύτερο κρυπτονόμισμα μετά το Bitcoin (BTC), σε επίπεδο κεφαλαιοποίησης.

Τα θετικά της πλατφόρμας είναι αρχικά το μεγάλο ποσοστό κεφαλαιοποίησης που διαθέτει, η υποστήριξή του από εταιρείες κολοσσούς , μεταξύ των οποίον η IBM, η Microsoft, η Amazon κ.α. Ένα ακόμη θετικό που διαθέτει η πλατφόρμα είναι η μεγάλη ζήτηση που δείχνουν προγραμματιστές για την ανάπτυξης της.

Ωστόσο εκτός από τα θετικά, το Ethereum έχει αρκετά μικρή ικανότητα διεκπεραίωσης αιτημάτων, η οποία σταματάει στα 20 ανά δευτερόλεπτο, πρόβλημα το οποίο ελαττώνει τις περιπτώσεις κλιμάκωσης των εφαρμογών του. Αρνητικό αποτελεί και η διαχείριση που διαθέτει από κεντρική αρχή, καθώς έχουν υπάρξει και περιπτώσεις κυβερνοεπιθέσεων και ειδικότερα μια από τις μεγαλύτερες που έχουν συμβεί στον κόσμο των κρυπτονομισμάτων. Ένα παράδειγμα επίθεσης έχει είδη αναφερθεί, στο υποκεφάλαιο εφαρμογής τεχνικών hard forking.

(Πολυτίδου, 2018)

(Ethereum, n.d.)

2.5.2 Hyperledger

HYPERLEDGER

Εικόνα 8. Hyperledger (x.x) [Το λογότυπο της κοινότητας Hyperledger]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.hyperledger.org

Πρόκειται περισσότερο για μία κοινότητα και λιγότερο για μια πλατφόρμα ανάπτυξης που ασχολείται με την ανάπτυξη ενός συνόλου framework, εργαλείων και βιβλιοθηκών για Blockchain που απευθύνονται στον κόσμο των επιχειρήσεων. Δεν αποτελεί ούτε κάποιο κρυπτονόμισμα, ούτε κάποιο Blockchain ούτε κάποια εταιρεία.

Είναι μία συνεταιριστική προσπάθεια ανοιχτού κώδικα, που ξεκίνησε το 2015 από το ίδρυμα Linux Foundation και έχει λάβει μεγάλες χρηματικές συνεισφορές για την ανάπτυξή του από την IBM, την Intel, την SAP Ariba κ.α. Αυτή τη στιγμή διαθέτει αρκετές από τις ποιο δημοφιλείς και καινοτόμες πλατφόρμες στο Blockchain μεταξύ των Hyperledger Avalon, Hyperledger Burrow, Hyperledger Cello, Hyperledger Fabric, Hyperledger Indy, Hyperledger Iroha, Hyperledger Sawtooth κ.α. καθώς και ένα μεγάλο σύνολο εργαλείων, μεταξύ των Hyperledger Caliper, Hyperledger Cello, Hyperledger Composer, Hyperledger Quilt κ.α. Η παραπάνω λίστα συνεχώς αυξάνεται και νέες δυνατότητες προστίθενται στην κοινότητα.

Οι χρήσεις της είναι στον τραπεζικό κόσμο, στα χρηματοπιστωτικά ιδρύματα, στις βιομηχανίες, στην ενέργεια, στην τεχνολογία και στην εφοδιαστική αλυσίδα. Επιχειρήσεις με την χρήση των εργαλείων που τους παρέχουν οι επιμέρους πλατφόρμες της κοινότητας, μπορούν να τις χρησιμοποιήσουν για να δώσουν λύσεις στα προβλήματά τους καθώς και να καλυτερεύσουν την αποτελεσματικότητα των διαδικασιών τους και να μειώσουν τα λειτουργικά τους έξοδα.

Όλες οι παραδοχές του Hyperledger, είτε πρόκειται για framework είτε για εργαλείο, βασίζονται σε μια καθορισμένη προσέγγιση κατά τη διαδικασία σχεδιασμού. Όλα τα Hyperledger είναι αρθρωτά, προσφέρουν μεγάλη επεκτασιμότητα σε όλα τα επίπεδα συστήματος-εφαρμογής και μεγάλο επίπεδο ασφαλείας. Στο επίπεδο αρχιτεκτονικής χρησιμοποιείται η Hyperledger Working Group(WG), ένα σύνολο κανόνων που έχει τα παρακάτω εννέα βασικά χαρακτηριστικά.

1. **Επίπεδο συναίνεσης** (Consensus Layer), υπεύθυνο για τη σύναψη συμφωνίας και την επιβεβαίωση της ορθότητας δεδομένων του συνόλου των συναλλαγών.
2. **Επίπεδο έξυπνων συμβολαίων** (Smart Contract Layer), υπεύθυνο για την εκτέλεση συναλλαγών και τον έλεγχο εγκυρότητάς τους με τη χρήση επιχειρηματικής λογικής (business logic).

3. **Επίπεδο επικοινωνίας** (Communication Layer), υπεύθυνο για τη μεταφορά peer-to-peer μηνυμάτων μεταξύ κόμβων που συνυπάρχουν σε ένα κοινόχρηστο καθολικό αρχείο συναλλαγών.
4. **Αφαίρεση αποθήκευσης δεδομένων** (Data Store Abstraction), επιτρέπει την χρήση δεδομένων από ένα μέρος σε άλλο της εφαρμογής.
5. **Αφαίρεση κρυπτογραφίας** (Crypto Abstraction), επιτρέπει την άμεση αλλαγή αλγορίθμων κρυπτογράφησης, χωρίς να επηρεάζεται το υπόλοιπο μέρος του δικτύου.
6. **Υπηρεσία Διαχείρισης Ταυτότητας (**Identity Services), χαρακτηριστικό το οποίο επιτρέπει την επιβεβαίωση και επικύρωση των χρηστών και των συστημάτων για την ύπαρξη εμπιστοσύνης εντός δικτύου.
7. **Υπηρεσίες πολιτικής** (Policy Services), σύστημα υπεύθυνο για τον καθορισμό και τη διαχείριση των πολιτικών του δικτύου. Η πολιτική έγκρισης, αλγορίθμων συναίνεσης και διαχείρισης χρηστών/ομάδων διαχειρίζονται από το σύστημα.
8. **Διασύνδεση Προγραμματισμού Εφαρμογών** (API), υπεύθυνο για την εύκολη αλληλεπίδραση μεταξύ χρήστη – εφαρμογής και Blockchain.
9. **Διαλειτουργικότητα** (Interoperation), υπεύθυνο για την αλληλεπίδραση μεταξύ διαφορετικών Blockchain.

(Hyperledger, 2018)

2.5.3 Hyperledger Sawtooth

Εικόνα 9. Hyperledger (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Hyperledger Sawtooth]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από sawtooth.hyperledger.org

Το Hyperledger Sawtooth είναι μια πλατφόρμα ανοιχτού κώδικα που αναπτύχθηκε από την Intel και βασίστηκε πάνω στην πλατφόρμα Hyperledger που προαναφέρθηκε. Πρόκειται για πλατφόρμα ανάπτυξης Blockchain που απευθύνεται στον εταιρικό κόσμο και στοχεύει στην ανάπτυξη εφαρμογών και δικτύων που βασίζονται στο δημόσιο καθολικό. Η σχεδίαση έγινε βάση της ιδέας για την ανάπτυξη ενός συστήματος που θα διατηρεί κατανεμημένο δημόσιο καθολικό, παρέχοντας και την ασφαλή χρήση των έξυπνων συμβολαίων. Με το ενσωματωμένο μοντέλο συναίνεσης που διαθέτει, είναι αρθρωτό, κλιμακούμενο και υποστηρίζει την λειτουργεία δικτύου με ή χωρίς άδεια (permissioned – permissionless).

Στις βασικές Blockchain πλατφόρμες υπάρχει μια ιδιαιτερότητα στην αρχιτεκτονική, ο πυρήνας και η εφαρμογή υπάρχουν και εκτελούνται από την ίδια πλατφόρμα, μια κατάσταση που μπορεί να αποφέρει μειωμένη ταχύτητα στη λειτουργεία της πλατφόρμας, προβλήματα ασφάλειας και ιδιαιτερότητες-δυσκολίες κατά την ανάπτυξή της. Όμως, το Hyperledger Sawtooth βασίζεται σε

μία διαφορετική αρχιτεκτονική, στην οποία ο πυρήνας και το επίπεδο εφαρμογής βρίσκονται στο δικό τους ξεχωριστό περιβάλλον. Με αυτή την τεχνική απλοποιείται η εφαρμογή και κατά τη χρήση της αλλά και κατά την ανάπτυξή της, καθώς ο ανάλογος χρήστης δεν θα χρειαστεί να γνωρίζει για τον τρόπο λειτουργίας και των δύο επιπέδων.

Η πλατφόρμα υποστηρίζει τις γλώσσες Python, JavaScript, Go, C++, Java, και Rust. Επιπλέον όπως όλες οι παραδοχές του Hyperledger, έτσι και εδώ παρέχεται RESTful API το οποίο απλοποιεί την ανάπτυξή της, εφαρμόζοντας την επικοινωνία επικυρωτή (*validator communication*) στο πρότυπο HTTP / JSON.

Το Sawtooth επιλύει αρκετά προβλήματα που υπήρχαν στα ιδιωτικά Blockchain. Συγκεκριμένα δεν υπάρχει κάποια κεντρική αρχή που ελέγχει την ανάπτυξη του δικτύου και έτσι αποκλείονται τα τυχόν προβλήματα ασφαλείας για τη διαρροή των δεδομένων. Όλοι οι κόμβοι κατά την ανάπτυξη μπορούν να δημιουργηθούν ευκολά με ξεχωριστή άδεια.

(Hyperledger - Sawtooth, χ.χ.)

2.5.4 Hedera Hashgraph

Εικόνα 10. Hedera (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Hedera Hashgraph]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.hedera.com

Το Hedera είναι η πρώτη και μοναδική για τη συγκεκριμένη στιγμή πλατφόρμα Blockchain, που χρησιμοποιεί το πρωτόκολλο συναίνεσης Hashgraph. Με το συγκεκριμένο πρωτόκολλο, η πλατφόρμα καταφέρνει να λειτουργεί με μεγάλη ασφάλεια και ταχύτητα ενώ παράλληλα δεν είναι αναγκαία η ύπαρξη υψηλής υπολογιστικής δύναμης για την ορθή λειτουργεία του δικτύου.

Το συγκεκριμένο πρωτόκολλο βασίζεται στο Proof-of-Stake (PoS) και οι εφαρμογές που έχει κυρίως αφορούν δημόσια δίκτυα. Η πλατφόρμα έχει το μεγαλύτερο δυνατό επίπεδο ασφάλειας (ABFT), παρέχοντας ταυτόχρονα υψηλές ταχύτητες για την πραγματοποίηση συναλλαγών, διατηρώντας παράλληλα και πολύ χαμηλή κατανάλωση δικτύου. Το Hashgraph, επιτυγχάνει υψηλή απόδοση στη διαδικασία της κρυπτογράφησης καθώς μπορεί να υποστηρίξει εύκολα τον υπολογισμό τουλάχιστον 10 χιλιάδων υπολογισμών κρυπτογράφησης ταυτόχρονα.

Το καθολικό αρχείο του δικτύου μοιάζει με το κλασσικό παράδειγμα blockchain που παρατηρούμε στα δίκτυα που λειτουργούν χωρίς άδεια, όπου είναι διαμοιρασμένο σε όλους τους συμμετέχοντες. Ωστόσο στους χρήστες διαμοιράζονται αντίγραφα του καθολικού αρχείου, καθώς το "πρωτότυπο" υπάρχει αποθηκευμένο σε κεντρικούς εξυπηρετητές από τους οποίους και διαμοιράζεται.

Χρησιμοποιείται για την κατασκευή αποκεντρωμένων εφαρμογών και μικρο-υπηρεσιών, μέσω ενός συνόλου API που διαθέτει και επιτρέπει την δημιουργία διαδικασιών (για τη δημιουργία λογαριασμών, για τη σύναψη έξυπνων συμβασιλέων, για την ενημέρωση του καθολικού αρχείου κ.α.) σχετικά εύκολα. Επιπλέον, το Hedera, παρέχει SDK (Software Development Kit, Κιτ Ανάπτυξης Λογισμικού) για τις γλώσσες Java, Javascript, GO και Typescript που κάνει την ανάπτυξη δικτύων ευκολότερη.

(Hedera, χ.χ)

2.5.5 Ripple

Εικόνα 11. Ripple (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Ripple]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.ripple.com

Το Ripple κυκλοφόρησε πρώτη φορά το 2012 και είναι ένα δίκτυο που στοχεύει στην ευκολία των παγκόσμιων συναλλαγών, δίνοντας σε χρηματοπιστωτικά ιδρύματα τη δυνατότητα να προσεγγίσουν ένα αξιόπιστο δίκτυο συνεργατών, προσφέροντας ταχύτητα στην πραγματοποίηση συναλλαγών και μηδενικές χρεώσεις. Όπως αναφέρεται και στην τεκμηρίωση (documentation) του Ripple, ο στόχος του είναι η εύκολη ανάπτυξη εφαρμογών που θα χρησιμοποιούν το XPR Ledger (μία ξεχωριστή παραδοχή του καθολικού αρχείου), χωρίς να χρειάζεται βαθιά γνώση από την ομάδα ανάπτυξης σε θέματα κρυπτογραφίας και κατανεμημένων συστημάτων. Επιπλέον πρόκειται για ένα κρυπτονόμισμα το οποίο χρησιμοποιείται και από τα μεγαλύτερα χρηματοπιστωτικά ιδρύματα του κόσμου όπως UBS, UniCredit κλπ.

Παρουσιάζει μια βασική διαφορά από τα υπόλοιπα νομίσματα Blockchain. Δεν απαιτείται η διαδικασία της εξόρυξης για την επιβεβαίωση των συναλλαγών. Η επιβεβαίωση αυτών γίνεται μέσω της χρήσης ενός διαφορετικού μοντέλου συναίνεσης και εξαλείφεται η χρήση τεράστιας ενεργειακής και υπολογιστικής ισχύς που θα χρειαζόταν άλλα δίκτυα για παρόμοια διαδικασία.

Αξίζει να σημειωθεί, το συγκεκριμένο δίκτυο έχει και τη δική του πλατφόρμα ανάπτυξης, την Xpring η οποία διαθέτει δικιά της βιβλιοθήκη (SDK Library) για αρκετές από τις διαδεδομένες γλώσσες προγραμματισμού και ειδικότερα για την Javascript (NodeJS), Java και τη Swift.

Τα θετικά της χρήσης του Ripple αφορούν την τεράστια ικανότητα του δικτύου που μπορεί να εκτελεί 1000 λειτουργείες ανά δευτερόλεπτο. Επιπλέον θετικό αποτελεί και η υποστήριξη από τράπεζες, χαρακτηριστικό που προσδίδει και κύρος στην πλατφόρμα. Η πλατφόρμα έχει ελάχιστα τέλη συναλλαγών και παρέχει τη δυνατότητα ακύρωσής τους.

Ωστόσο στο Ripple πάνω από το 60% των συνολικών XRP που υπάρχουν, κατέχονται από την εταιρεία που το διαχειρίζεται, επομένως έχουν πάνω από το 51% του δικτύου που χρειάζεται για τον πλήρη έλεγχο των Blockchain.

Τέλος, αξίζει να σημειωθεί και η σημαντικότερη διαφορά του σε σχέση με λοιπά κρυπτονομίσματα. Το ripple είναι ένα κρυπτονόμισμα το οποίο έχει ήδη εξορυχθεί και για αυτό το λόγο τα κίνητρα για τη λειτουργεία κόμβων στο δίκτυο, είναι ελάχιστα έως και μηδαμινά. Επομένως, εταιρείες που το χρησιμοποιούν όπως τράπεζες, θα πρέπει να παρέχουν τους κόμβους επικύρωσης. Η πλατφόρμα λόγω της συγκεκριμένης ιδιαιτερότητας ύπαρξης ελάχιστων κόμβων για τη λειτουργεία της, δεν μπορεί να θεωρηθεί αποκεντροποιημένη.

(XRP, χ.χ.)

2.5.6 Quorum

Εικόνα 12. Consensys (x.x) [Το λογότυπο της πλατφόρμας ανάπτυξης Quorum]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.goquorum.com

Το Quorum είναι μια πλατφόρμα ανοιχτού κώδικα που αναπτύχθηκε από την JP Morgan, έχοντας ως βάση το Ethereum, η οποία δημιουργήθηκε με διαδικασία fork. Η πλατφόρμα αυτή προσθέτει στην ήδη εξελιγμένη πλατφόρμα, επιπλέον δυνατότητες υποστήριξης των αναγκών που έχουν οι επιχειρήσεις.

Λόγω της αρχιτεκτονικής της πλατφόρμας, δίνεται η δυνατότητα στους δημιουργούς για την επιλογή και διαφορετικών αλγορίθμων συναίνεσης. Από πλευράς ανάπτυξης, η πλατφόρμα προσφέρει δικό της framework, το Cakeshop, το οποίο έρχεται και με περιβάλλον διεσπάρης κάνοντας την χρήση της ευκολότερη και αρκετά πιο γρήγορη από τις υπόλοιπες πλατφόρμες. Χρησιμοποιεί τη γλώσσα προγραμματισμού Java και ένα framework της Javascript, το NodeJs. Μπορεί να χρησιμοποιηθεί σε όλα τα δίκτυα που θα βασίζονται στο Ethereum και παρέχει τα απαραίτητα εργαλεία για τη διαχείριση ενός τοπικού κόμβου Blockchain, τη δημιουργία clusters, την εύκολη και γρήγορη απεικόνιση της κατάστασης που βρίσκεται η αλυσίδα καθώς και την υποστήριξη της λειτουργίας έξυπνων συμβολαίων.

Σύμφωνα με τον κατασκευαστή της πλατφόρμας, είναι ιδανική για οποιαδήποτε εφαρμογή χρειάζεται υψηλή ταχύτητα για την εκτέλεση ιδιωτικών συναλλαγών εντός ενός ιδιωτικού δικτύου Blockchain. Λόγω του ότι πρόκειται για ένα δίκτυο Blockchain που για τη συμμετοχή χρηστών είναι αναγκαία η παροχή αδείας, η χρήση του αλγορίθμου συναίνεσης PoW, δεν κρίνεται η καταλληλότερη λόγω της τεράστιας ενέργειας που χρειάζεται ο συγκεκριμένος αλγόριθμος. Για αυτό το λόγο η συγκεκριμένη πλατφόρμα χρησιμοποιεί αρκετά εξιδεικευμένους και διαφορετικούς αλγορίθμους συναίνεσης από αυτούς που έχουν αναφερθεί, κυρίως τον RAFT και τον IBFT(Istanbul Byzantine Fault Tolerant*).* Με τον αλγόριθμο RAFT, όταν εμφανίζεται μια νέα συναλλαγή στο δίκτυο, αυτή αποστέλλεται σε έναν κεντρικό κόμβο, ο οποίος με τη σειρά του

αποστέλλει τη συναλλαγή σε όλους τους υπόλοιπους κόμβους ζητώντας επιβεβαίωση αυθεντικότητας της συναλλαγής, χωρίς να χρειάζεται καμία επικοινωνία των κόμβων μεταξύ τους. Ο IBFT είναι παρόμοιος με τον RAFT ωστόσο γίνεται χρήση αρκετών κόμβων οι οποίοι χαρακτηρίζονται κεντρικοί.

Με την χρήση των αλγορίθμων που αναφέρθηκαν, το Quorum διαθέτει μεγάλη δυνατότητα κλιμάκωσης, ταχύτητα στις συναλλαγές και επικοινωνία με εγκεκριμένους κόμβους για τη διασφάλιση και το απόρρητο λειτουργειών. Αν και με τη χρήση κεντρικών κόμβων χάνεται το πλεονέκτημα του Blockchain για τα αποκεντροποιημένα συστήματα, αποτελεί μια αρκετά καλή λύση για την εισαγωγή λύσεων Blockchain στον τραπεζικό κλάδο.

(Quorum, 2018)

2.5.7 OpenChain

Εικόνα 13. OpenChain (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης OpenChain]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.openchain.org

Το OpenChain όπως δηλώνει και το όνομα του (OpenChain) πρόκειται για λογισμικό ανοιχτού κώδικα που προσφέρει λύσεις στον τομέα του Blockchain. Πρόκειται για λογισμικό που στοχεύει σε επιχειρήσεις που ως κύριο έργο έχουν την έκδοση και διαχείριση ψηφιακών στοιχείων ενεργητικού, προσφέροντας παράλληλα μεγάλο επίπεδο επεκτασιμότητας για την ικανοποίηση κάθε πιθανής ανάγκης. Οποιοδήποτε θέλει μπορεί να δημιουργήσει το δικό του δίκτυο OpenChain εντός δευτερολέπτων Σαν πλατφόρμα, εκτός από την ψηφιακή υπογραφή για την επικύρωση των συναλλαγών, παρουσιάζει βασικές διαφορές από άλλες που βασίζονται στην τεχνολογία του Blockchain.

Χρησιμοποιεί την αρχιτεκτονική χρήστη-εξυπηρετητή (*client-server*) που είναι πιο αποδοτική και σταθερή από την peer-to-peer που κυρίως χρησιμοποιείται στα Blockchain. Αρχική διαφορά, είναι ότι υπάρχει ένας διαχειριστής του συστήματος ο οποίος καθορίζει και τους κανόνες που θα ισχύουν στο δίκτυο. Η επιβεβαίωση των συναλλαγών γίνεται σε πραγματικό χρόνο από κεντρικούς διακομιστές ενώ για τη δημιουργία νέων block δεν είναι απαραίτητη η τεχνική της εξόρυξης, κάνοντας το δίκτυο δωρεάν και άμεσο. Ίσως το πιο “δυνατό” χαρακτηριστικό του OpenChain, είναι η δυνατότητα λειτουργίας πολλαπλών δικτύων εντός ενός οργανισμού καθώς και η δυνατότητα πλήρους επικοινωνίας και αλληλεπίδρασης όλων των δικτύων μεταξύ τους. Η πλατφόρμα ανάπτυξης, προσφέρεται για τις γλώσσες C# και Javascript και υπάρχει ένα μεγάλο κείμενο τεκμηρίωσης που βοηθά στην κατανόηση του OpenChain, κάθε νέο χρήστη που ενδιαφέρεται για την ανάπτυξη ενός δικτύου Blockchain βασισμένο σε αυτή την πλατφόρμα.

(OpenChain, n.d.)

2.5.8 Codra

Εικόνα 14. Corda (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης Corda]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.corda.net

Πρόκειται για λογισμικό ανοιχτού κώδικα που δεν παρέχει κάποιο κρυπτονόμισμα. Αναπτύχθηκε και διαχειρίζεται από την κοινοπραξία λογισμικού R3, για καταγραφή, παρακολούθηση και συγχρονισμό χρηματοοικονομικών συμφωνιών μεταξύ χρηματοπιστωτικών ιδρυμάτων που λειτουργούν κάτω από κοινούς όρους και κανόνες. Είναι ένα ιδιωτικό δίκτυο το οποίο διασφαλίζει ότι τα δεδομένα διαμοιράζονται μόνο στα άτομα που απευθύνονται. Στην πράξη αποδείχθηκε όμως ότι μπορεί να έχει εφαρμογές και σε ευρύτερο πεδίο. Ο σκοπός που δημιουργήθηκε αφορά στην μείωση των κοστοβόρων επιχειρηματικών διαδικασιών και για τον ορθολογισμό επιχειρηματικών δραστηριοτήτων.

Το Corda κάνει χρήσεις ιδιαίτερων αλγορίθμων συναίνεσης για την επικύρωση συναλλαγών και διατήρησης της ορθής λειτουργίας του δικτύου, ενώ παράλληλα δίνει και τη δυνατότητα επιλογής του ανάλογου αλγορίθμου.

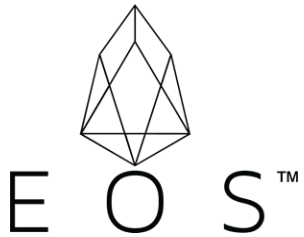
Στους συγκεκριμένους αλγορίθμους, θεσμοθετούνται κάποιοι κόμβοι που λειτουργούν σαν συμβολαιογράφοι και διαχειρίζονται τα έξυπνα συμβόλαια καθώς και την πρόοδο που αυτά έχουν. Το λογισμικό διαθέτει δύο βασικά χαρακτηριστικά των μοντέρνων δικτύων Blockchain, τα έξυπνα συμβόλαια και την λειτουργία χρονοσήμανσης εγγράφων-διαδικασιών. Επιπλέον εμπεριέχει ένα ακόμη χαρακτηριστικό που ονομάζεται πλαίσιο ροής (flow framework) και απλουστεύει τη διαδικασία σύνταξης σύνθετων πρωτοκόλλων μεταξύ πολλών μερών, που πρόκειται να λάβουν μέρος σε μία συναλλαγή. Τέλος, ιδιαίτερο χαρακτηριστικό για τη συγκεκριμένη πλατφόρμα ανάπτυξης αποτελεί και η έλλειψη παρουσίας κάποιου κρυπτονομίσματος.

Ήδη μεγάλα χρηματοπιστωτικά ιδρύματα όπως η HSBC, η ING, η BBVA και η Βασιλική Τράπεζα της Σκωτίας το έχουν χρησιμοποιήσει για τις εμπορικές συναλλαγές τους, όπως και άλλες επιχειρήσεις το χρησιμοποιούν, στον κόσμο της εφοδιαστικής αλυσίδας, της ενέργειας, της υγείας κ.α.

Η πλατφόρμα είναι ανεπτυγμένη στη γλώσσα Kotlin και Java, ενώ παράλληλα τρέχει στο Java Virtual Machine. Αυτή η τελευταία ιδιαιτερότητα, δίνει την δυνατότητα στην πλατφόρμα να μπορεί να χρησιμοποιήσει ένα τεράστιο εύρος βιβλιοθηκών που ήδη υπάρχουν για την πλατφόρμα της Java.

(R3, n.d.)

2.5.9 EOS.IO



Εικόνα 15. EOS.IO (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης EOS.IO]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.eos.io

Πρόκειται για μια νέα σχετικά πλατφόρμα που δημιουργήθηκε από την εταιρεία block.one και εμφανίστηκε το 2018 για πρώτη φορά. Η συγκεκριμένη πλατφόρμα, χρησιμοποιεί μία διαφορετική προσέγγιση στην αρχιτεκτονική σχεδίαση Blockchain συστημάτων σε σύγκριση με τα κλασσικά. Επιτρέπει σε επιχειρήσεις τη δημιουργία και ανάπτυξη εφαρμογών που βασίζονται σε πρωτόκολλο Blockchain ενώ παρέχει υψηλή απόδοση και ασφάλεια σε κάθε υλοποίηση.

Το EOS.IO, δίνει τη δυνατότητα για κατακόρυφη και οριζόντια κλιμάκωση αποκεντρωμένων εφαρμογών. Χρησιμοποιώντας μια φιλοσοφία σαν λειτουργικό σύστημα, αφήνει εφαρμογές να χτίζονται πάνω σε συγκεκριμένα συστήματα ενώ παράλληλα παρέχει και τη δυνατότητα δημιουργίας και διαχείρισης λογαριασμών για την καταγραφή και τον έλεγχο ταυτότητας χρηστών. Εκτός από το τελευταίο, το EOS.IO προσφέρει επίσης βάσεις δεδομένων και ασύγχρονη επικοινωνία. Μέσω της συγκεκριμένης αρχιτεκτονικής προσέγγισης, ένα σύστημα βασισμένο στο EOS.IO μπορεί να εκτελεί εκατομμύρια συναλλαγές ανά δευτερόλεπτο και να επιτρέπει την εύκολη ανάπτυξη και συντήρηση αποκεντρωμένων εφαρμογών, στο πλαίσιο ενός ιδιωτικού Blockchain που λειτουργεί με την παροχή άδειας για συμμετοχή στο δίκτυο.

(EOS.IO, 2018)

2.5.10 BigChainDB

Εικόνα 16. BigChainDB (χ.χ.) [Το λογότυπο της πλατφόρμας ανάπτυξης BigChainDB]. Ανακτήθηκε 10 Σεπτεμβρίου 2020, από www.bigchaindb.com

Πρόκειται για λογισμικό που κρατάει κύρια χαρακτηριστικά του Blockchain, όπως αποκέντρωση, μεταβλητότητα και διαχείριση περιουσιακών στοιχείων και τα χρησιμοποιεί για να τα συνδέσει με τα χαρακτηριστικά μιας αρκετά εξελιγμένης τεχνολογίας, τις βάσεις δεδομένων. Ειδικότερα με τον υψηλό ρυθμό συναλλαγών, το μικρό χρόνο καθυστέρησης (low-latency) και την δυνατότητα χρήσης ευρετηρίων (indexes) που διαθέτει, το BigChainDB αποτελεί μια καινοτόμα εναλλακτική επιλογή στην επιλογή πλατφόρμας ανάπτυξης. Σαν λογισμικό, δημοσιεύτηκε πρώτη φορά τον Φεβρουάριο του 2016. Πρόκειται για λογισμικό ανοιχτού κώδικα και από τη στιγμή της δημοσίευσής του, συνεχώς αναβαθμίζεται και γίνεται προσθήκη νέων δυνατοτήτων σε αυτό.
(BigchainDB GmbH, Berlin, Germany, 2018)

3. Τομείς Χρήσης και Διαδεδομένες Εφαρμογές

Όπως έχει αναφερθεί αρκετές φορές στην εργασία, το Blockchain μπορεί να έχει εφαρμογές για την παροχή λύσεων σε αρκετούς ιδιωτικούς και δημοσίους οργανισμούς. Όλο και περισσότερα κράτη χρησιμοποιούν το Blockchain για την καλύτερη διαχείριση πόλεων, την συνεχή εξυπηρέτηση πολιτών όλο το εικοσιτετράωρο καθώς και για την διακίνηση και αποθήκευση απόρρητων εγγράφων. Στον ιδιωτικό τομέα επιχειρήσεις στον κόσμο της εφοδιαστικής αλυσίδας, των νομικών υπηρεσιών, της υγείας, των πνευματικών δικαιωμάτων, των χρηματοοικονομικών και επενδύσεων καθώς και σε πολλούς άλλους τομείς, μπορούν να χρησιμοποιήσουν το Blockchain.

Ειδικότερα, παραδείγματα επενδύσεις κρατών και φορέων αποτελεί η ΕΕ που δημιούργησε το EU Blockchain Observatory & Forum για να βοηθήσει στην ερευνά και ανάπτυξη της καινοτομίας της Ευρώπης σαν έναν παγκόσμιο ηγέτη τεχνολογίας. Επιπλέον, το European Horizon 2020 Program επενδύει επιπλέον 300 εκατομμύρια σε project που βασίζονται στο Blockchain. Στις επόμενες 6 ενότητες παρουσιάζονται παραδείγματα χρήσης υλοποιημένων εφαρμογών Blockchain στον σημερινό κόσμο.

3.1 Κυβερνήσεις και Δημόσιος Τομέας

Αν και στον συγκεκριμένο τομέα το Blockchain μπήκε τελευταία, δείχνει τις ικανότητες που έχει καθώς όλο και περισσότερα κράτη και φορείς αυτών το εμπιστεύονται και επενδύουν σε καινοτόμες λύσεις που βασίζονται στην συγκεκριμένη τεχνολογία.

3.1.1 E-Esthonia

Η Εσθονία ήταν από τις πρώτες χώρες που πειραματιζόταν με την τεχνολογία ήδη από το 2008, όταν και έκανε τα πρώτα της βήματα. Σήμερα η κυβέρνηση έχει δημιουργήσει μια πλατφόρμα την E-Esthonia, η οποία διαθέτει πάνω από το 99% των κρατικών υπηρεσιών που θα χρειαστεί ένας πολίτης άμεσα διαθέσιμο στο διαδίκτυο, προσβάσιμο από κάθε είδους συσκευή με πρόσβαση σε αυτό. Ήδη πάνω από το 44% του πληθυσμού χρησιμοποίει την πλατφόρμα για ηλεκτρονική ψηφοφορία στη διαδικασία των εκλογών. Σημαντικά ποσοστά είναι και το 98% των φορολογικών δηλώσεων που γίνονται online καθώς και ότι το 98% του πληθυσμού της χώρας έχουν ψηφιακή ταυτότητα. Η Εσθονία επενδύει συνεχώς στο Blockchain και σε καινοτόμες υπηρεσίες βάζοντας τέλος στην γραφειοκρατία και στους αργούς ρυθμούς που ταλανίζουν τους κρατικούς μηχανισμούς.

3.1.2 Smart Dubai

Η κυβέρνηση των Ηνωμένων Αραβικών Εμιράτων (ΗΑΕ) εργάζεται ήδη με κάτι αρκετά

πρωτότυπο. Δημιούργησε μια πλατφόρμα με όνομα Smart Dubai και στοχεύει να κάνει το 2020 το Ντουμπάι την πρώτη έξυπνη πόλη του κόσμου.

Στόχος του προγράμματος είναι η αξιοποίηση του Blockchain και η ψηφιοποίηση κρατικών διαδικασιών σε ομοσπονδιακό επίπεδο. Με την υιοθέτηση της τεχνολογίας, εκτιμάτε ότι τα ΗΑΕ θα σώσουν 11 δις σε συναλλαγές και έγγραφα, 398 εκατομμύρια έντυπα ετησίως και 77 εκατομμύρια ώρες εργασίας ετησίως. Επιπλέον θα μειωθούν κατά 1,6 δισεκατομμύρια τα χιλιόμετρα οδήγησης καθώς οι πολίτες θα μπορούν να κάνουν τις απαραίτητες διαδικασίες από το σπίτι. Είναι φανερό λοιπόν ότι πέρα από τα θετικά που έχει για την διευκόλυνση του ανθρώπου, υπάρχουν και θετικά και για την προστασία του περιβάλλοντος.

3.2 Εφοδιαστική αλυσίδα

Μιας και μιλάμε για ένα παγκόσμιο τομέα όπου για την εξυπηρέτηση πελατών συνεργάζονται μεγάλος αριθμών επιχειρήσεων και εργαζομένων, οι ανάγκες για τη διακίνηση αγαθών στον τομέα των logistics γίνονται όλο και πιο σύνθετες. Ο βασικός τομέας στα logistics που θα μπορούσε να έχει μεγάλη επίδραση είναι το παγκόσμιο εμπόριο. Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί από την DHL (DHL, 2020), η χρήση συστημάτων που εξαλείφουν τα εμπόδια στην εφοδιαστική αλυσίδα μπορεί να συμβάλει στην αύξηση του παγκόσμιου ΑΕΠ κατά 5% και την συνολική αύξηση του παγκόσμιου εμπορίου κατά 15%.

3.2.1 Treum

Το Treum αναπτύχθηκε από την εταιρεία ConsenSys με σκοπό να φέρει το Blockchain στον κόσμο της εφοδιαστικής αλυσίδας. Η πλατφόρμα βασισμένη πάνω στο Ethereum φέρνει διαφάνεια, ιχνηλασιμότητα και εμπορευσιμότητα στην εφοδιαστική αλυσίδα. Η διαφάνεια παρέχει τη δυνατότητα στις εταιρείες να μοιράζονται με τους πελάτες τους τα απαραίτητα έγγραφα ανά πάσα στιγμή με σκοπό τη βελτίωση της εμπιστοσύνης και της αυθεντικότητας των προϊόντων-υπηρεσιών που παρέχει μια εταιρεία. Επιπλέον, μέσω της ιχνηλασιμότητας παρέχεται η δυνατότητα παρακολούθησης της πορείας των προϊόντων τους από το πρωτογενές στάδιο παραγωγής έως και το στάδιο της πώλησης.

Τέλος, με την εμπορευσιμότητα παρέχεται η δυνατότητα στους πελάτες να διαχειρίζονται σε πραγματικό χρόνο τα περιουσιακά τους στοιχεία. Οι ίδιοι μπορούν να τα κρατήσουν, να τα ανταλλάξουν ή να αποκτήσουν νέα και όλο αυτά οποιαδήποτε στιγμή οι ίδιοι θελήσουν.

(Treum, χ.χ.)

3.2.2 Η περίπτωση της Walmart

Η Walmart μία από τις μεγαλύτερες εταιρείες στις ΗΠΑ στον τομέα του λιανικού εμπορίου, αποτελεί πρωτοπόρο για την χρήση τεχνολογίας Blockchain στον κλάδο της. Ήδη από το 2016,

μαζί με την IBM έχουν υπογράψει συνεργασία για την απόκτηση ενός συστήματος που θα βοηθήσει στην καλύτερη και ταχύτερη ιχνηλασιμότητα των προϊόντων που διακινεί μέσω των καναλιών της η εταιρεία. Συγκεκριμένα η λύση που ετοιμάζεται από την IBM αφορά στον έλεγχο της διακίνησης φαγώσιμων προϊόντων. Με αυτό το σύστημα, η Walmart θα είχε στα χέρια της ένα εργαλείο που θα παρακολουθεί σε πραγματικό χρόνο την πορεία ενός προϊόντος από τον πρωτογενή τομέα έως την κατανάλωση.

Επιπλέον, η εταιρεία εκτός της αυξημένης ορατότητας για την διακίνηση των εμπορευμάτων, μπορεί να επεκτείνει το σύστημα της για τον έλεγχο εξάπλωσης τροφικών ασθενειών με στόχο τον περιορισμό δαπανηρών τέτοιων ανακλήσεων. Η δυνατότητα παροχής Blockchain λύσεων έχει αρχίσει και εφαρμόζεται ήδη από το 2019, όπου η Walmart το χρησιμοποίησε για την ιχνηλασιμότητα και τον έλεγχο διανομής μαρουλιών από όλους τους παραγωγούς της.

(Infopulse, 2019)

3.3 Νομικές Υπηρεσίες

Σίγουρα ένας ασυνήθιστος τομέας για την τεχνολογία, ωστόσο το Blockchain φέρνει και εδώ καινοτόμες λύσεις, εξασφαλίζοντας διαφάνεια και ταχύτερη διεκπεραίωση χρονοβόρων διαδικασιών. Οι εργαζόμενοι στον τομέα αξιοποιούν την τεχνολογία με τα έξυπνα συμβόλαια που παρέχει, μειώνοντας κατά πολύ τον χρόνο που θα χρειαζόταν για την συλλογή των απαραίτητων εγγράφων, τη σύνταξη και εξατομίκευση κάθε συμβολαίου μειώνοντας τα λειτουργικά έξοδα της επιχείρησης και το σύνολο των χρημάτων που θα έχει να πληρώσει ένας πελάτης.

3.3.1 Open Law

Το Open Law είναι μια Blockchain εφαρμογή που στοχεύει στη υλοποίηση χρήσεων Blockchain στον τομέα των νομικών υπηρεσιών, ειδικότερα στην δημιουργία και εκτέλεση νομικών συμφωνιών. Ο στόχος του Open Law είναι η δημιουργία μιας πλατφόρμας παραδοσιακών νομικών συμφωνιών αλλά με τη χρήση των έξυπνων συμβολαίων, παρέχοντας παράλληλα ένα σύστημα Blockchain με φιλικό περιβάλλον διεπαφής (*GUI*) για όλους τους χρήστες του. Οι χρήστες της εφαρμογής μπορούν να εμπλακούν πιο άμεσα και γρήγορα στις εκάστοτε νομικές διαδικασίες υπογράφοντας συμβόλαια και αποθηκεύοντας τα με πολύ ασφαλή τρόπο .

Οι δημιουργοί του έχουν δημιουργήσει έναν τύπο mark-up γλώσσας, η οποία δίνει την δυνατότητα στην εφαρμογή να μεταφέρει στον περιβάλλον των Blockchain όλες τις πιθανές νομικές συμφωνίες.

(OpenLaw, χ.χ.)

3.4 Τράπεζες και χρηματοπιστωτικά Ιδρύματα

Όπως είναι γνωστό ο τραπεζικός κόσμος διαθέτει μεγάλα ποσά χρημάτων και αποτελεί στόχο πολλών ανθρώπων, οι οποίοι προσπαθούν να λάβουν χρήματα μέσω έκνομων ενεργειών. Στις έως

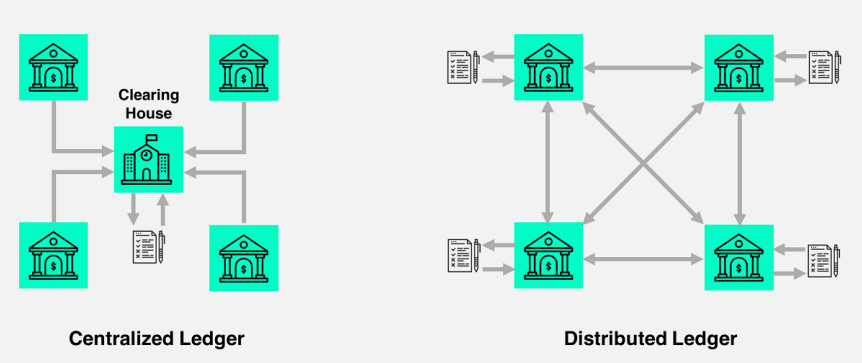
τώρα ψηφιακές λύσεις e-banking, τα τραπεζικά ιδρύματα δαπανούν μεγάλα ποσά για τη διατήρηση μεγίστης ασφάλειας, παρόλα αυτά έχουν υπάρξει περιπτώσεις όπου συστήματα τραπεζών κατάφεραν να παραβιαστούν και χρήματα μεγάλης αξίας έχουν χαθεί. Το Blockchain θα μπορούσε να φέρει λύση στα συγκεκριμένα προβλήματα ασφαλείας των τραπεζών αλλά ίσως και σε περισσότερους τομείς.

Στα έως τώρα τραπεζικά συστήματα τα δεδομένα είναι σχετικά ευάλωτα καθώς είναι αποθηκευμένα σε έναν κεντρικό υπολογιστή. Επομένως εάν κάποιος καταφέρει και αποκτήσει πρόσβαση σε αυτόν, αυτομάτως λαμβάνει πρόσβαση και σε όλα τα δεδομένα που υπάρχουν στο συγκεκριμένο σύστημα.

Το Blockchain μπορεί να φέρει λύση σε αυτό, καθώς ένα από τα κύρια χαρακτηριστικά του είναι η αποκέντρωση. Έτσι δεν είναι απαραίτητο όλα τα δεδομένα της τράπεζας να είναι αποθηκευμένα σε ένα σύστημα, μπορούν να είναι διαμοιρασμένα σε ένα σύνολο υπό-συστημάτων. Επιπλέον λύση που φέρνει η συγκεκριμένη τεχνολογία είναι και η ύπαρξη της δυνατότητας χρονοσήμανσης και ελέγχου κάθε συναλλαγής σε πραγματικό χρόνο, κάνοντας τα δεδομένα αναλλοίωτα και εύκολο τον εντοπισμό εκνόμων ενεργειών. Επιπλέον γραφειοκρατικές διαδικασίες όπως για την επικαιροποίηση στοιχείων, τη δημιουργία νέων λογαριασμών κ.α. θα μπορούσαν να μειωθούν περεταίρω σε χρόνο με τη χρήση του Blockchain. Ωστόσο, ο βασικότερος τομέας που φαίνεται ότι έχει χρήση η συγκεκριμένη τεχνολογία είναι στις συναλλαγές. Σήμερα παρατηρούμε ότι τα δίκτυα της τράπεζας αργούν έστω και για δευτερόλεπτα στην εκτέλεση των συναλλαγών και πολλές φορές ολόκληρο το σύστημα της τράπεζες πέφτει με αποτέλεσμα καμία συναλλαγή να μην μπορεί να εξυπηρετηθεί. Με τη χρήση του, οι εταιρείες θα μειώσουν σημαντικά τον χρόνο πραγματοποίησης συναλλαγών και θα μειώσουν τις σχέσεις που έχουν με τρίτες εταιρείες που συνεργάζονται για την άρτια λειτουργία των πληροφοριακών τους συστημάτων. Τέλος σημαντικό επιπλέον πλεονέκτημα που φέρνει το Blockchain στον χώρο της τραπεζικής είναι και τα έξυπνα συμβόλαια, τα οποία μειώνουν στο ελάχιστο το κόστος και τον χρόνο που χρειάζεται για την δημιουργία οποιουδήποτε συμβολαίου σχετικό με την τράπεζα,

Παρόλα αυτά τα τραπεζικά ιδρύματα είναι ακόμη διστακτικά για μια τέτοια μετάβαση και λίγοι είναι αυτοί που κάνουν το βήμα. Ο βασικός δισταγμός των τραπεζών ξεκινά από το ότι δεν θα υπάρχει κάποια κεντρική αρχή για τον έλεγχο των διαδικασιών καθώς και πως τα πιο διαδεδομένα και αποδεδειγμένα ότι λειτουργούν σωστά δίκτυα Blockchain, απαιτούν τεράστια ηλεκτρική και επεξεργαστική ισχύ, κάτι που προς το παρόν οι τράπεζες με τον εξοπλισμό που διαθέτουν δεν μπορούν να καλύψουν.

Στην *Εικόνα* 16 γίνεται μία σύγκριση του τρόπου που εκτελείται μια συναλλαγή σήμερα (αριστερά) και του τρόπου που μπορεί να πραγματοποιηθεί μέσω Blockchain (δεξιά). Έστω ότι πραγματοποιείται μια Χ συναλλαγή μεταξύ δύο αντισυμβαλλόμενων, του Α και του Β. Στα έως τώρα γνωστά συστήματα για να θεωρηθεί έγκυρη μια συναλλαγή από τον Α στον Β πρέπει να λάβει και την διαπίστωση ότι πρόκειται για μια νόμιμη και πραγματοποιήσιμη συναλλαγή από μια κεντρική αρχή. Από την άλλη όταν χρειάζεται να γίνει μεταφορά από τον Α στον Β, "επικοινωνούν" μεταξύ τους. Η συναλλαγή ελέγχεται από τους κανόνες που έχουν θεσπιστεί στο δίκτυο, αν συμφωνεί με όλα, μέσω της ψηφιακής υπογραφής εγκρίνεται και πραγματοποιείται χωρίς την ανάγκη ύπαρξης κεντρικής ελεγκτικής αρχής, όπως στο προηγούμενο σύστημα.



Εικόνα 17. [Απεικόνιση του αποκεντρωμένου καθολικού σε περιβάλλον τράπεζας]. (χ.χ). Ανακτήθηκε 3 Σεπτεμβρίου, από https://coinrevolution.com/what-is-a-distributed-ledger/

3.5 Φιλανθρωπικοί οργανισμοί

Οι φιλανθρωπικοί οργανισμοί συχνά έρχονται αντιμέτωποι με εμπόδια όπως τη μη ύπαρξη διαφάνειας, λογοδοσίας και του τρόπου αποδοχής δωρεών. Πολλές φορές γίνονται διαμαρτυρίες για τη μη ορθή χρήση των δωρηθέντων χρημάτων καθώς και για την σπατάλη αυτών σε διαφορετικούς σκοπούς από αυτούς που αναφέρονται στην ανάλογη εκστρατεία. Η χρήση της τεχνολογίας του Blockchain προσφέρει μια διαφορετική και καινοτόμα προσέγγιση στα φιλανθρωπικά ιδρύματα με την χρήση αποκεντρωμένων και άμεσων συναλλαγών που βοηθούν τα ιδιά στην πιο αποτελεσματική λήψη και διαχείριση δωρεών συνολικά. Με το Blockchain ο κλάδος των φιλανθρωπιών πρόκειται να αναβαθμιστεί καθώς θα παρέχεται πλήρης διαφάνεια, μειωμένα λειτουργικά έξοδα για τις ΜΚΟ, αποκεντρωμένα συστήματα που θα λειτουργούν ανεξάρτητα, καθώς και μειωμένη φορολόγηση στο έπακρον, αφού δωρεές που γίνονται με κρυπτονομίσματα δεν υπόκεινται σε φορολογία.

3.5.1 Bithope

Το Bithope είναι βουλγάρικος ΜΚΟ με τεχνολογία βασισμένη στο Blockchain που χρησιμοποιεί μόνο κρυπτονομίσματα για την ενίσχυση των εκστρατειών που βρίσκονται στον ισότοπό του, https://bithope.org/ . Πρόκειται για έναν από τους ελάχιστους ΜΚΟ που υποστηρίζουν δωρεές μόνο με την καταβολή κρυπτονομισμάτων, διατηρώντας πάνω από όλα την ανωνυμία των δωρητών. Πάνω από το 95% των χρημάτων που τους κατατίθεται πάει απευθείας στον τελικό δικαιούχο κάθε εκστρατείας. Το υπόλοιπο ποσοστό κρατείτε από το Bithope για την επιπλέον ενίσχυση και λοιπών εκστρατειών που τρέχουν στο site του την παρούσα χρονική στιγμή. Το συγκεκριμένο ίδρυμα συνεργάζεται με εδραιωμένες ΜΚΟ, που για αρκετά χρόνια έχουν αποδείξει επαγγελματισμό, προσφέροντας παράλληλα ένα αίσθημα σιγουριάς, ότι τα χρήματα που δωρίζονται θα πάνε στον πραγματικό δικαιούχο και δεν θα βρεθούν σε κάποιον τρίτο.

(What is BitHope, χ.χ.)

3.5.2 Binance Charity

Το Binance Charity είναι ένας ΜΚΟ με βασικό στόχο την επίτευξη ενός βιώσιμου περιβάλλοντος για όλους μας, με τη χρήση της τεχνολογίας Blockchain. Οι στόχοι της πλατφόρμας αφορούν στην βελτιστοποίηση της διαφάνειας που υπάρχει στους φιλανθρωπικούς οργανισμούς, στην ανάπτυξη των κρυπτονομισμάτων και για την χρήση τους σε περιπτώσεις που αφορούν δωρεές καθώς και στην αυξημένη ταχύτητα για την επίτευξη βιώσιμης ανάπτυξης για τον πλανήτη μας.

Το Binance δημιουργεί διαφάνεια σε περιβάλλοντα φιλανθρωπικών οργανισμών καθώς η ροή των χρημάτων μεταξύ του ίδιου και των δωρητών είναι διαφανής και αποτελεσματική. Η ομάδα ανάπτυξης εργάζεται συνεχώς για την όλο και πιο σωστή κατανόηση των αναγκών που έχει κάθε τόπος για την επίλυση συγκεκριμένων προβλημάτων.

(binance.charity, χ.χ.)

3.6 Προσωπικά Δεδομένων

3.6.1 Po.et

Το Po.et είναι ένα αποκεντρωμένο πρωτόκολλο ιδιοκτησίας, ανακάλυψης περιεχομένου και δημιουργίας εσόδων στα social media. Η συγκεκριμένη εφαρμογή, διαθέτει ένα ανοιχτό σε όλους καθολικό αρχείο, στο οποίο καταγράφονται με τη λογική του Blockchain (αμεταβλητότητας) πληροφορίες σχετικά με το δημιουργικό περιεχόμενο χρηστών. Η εφαρμογή παρέχει παράλληλα διαλειτουργικότητα και δυνατότητα χρήσης πρωτοκόλλων που έχουν εφαρμογή σε σύγχρονα πρότυπα της βιομηχανίας.

Η πλατφόρμα διαθέτει βασικά χαρακτηριστικά:

1) **Απόδοση**, παρέχονται καινοτόμοι τρόποι αναφοράς οποιονδήποτε περιουσιακών στοιχείων περιεχομένου σε ολόκληρο το δίκτυο, για τη δημιουργία έγκυρων αξιώσεων.
2) **Δημιουργία κερδών,** επεκτείνει τις δυνατότητες για δημιουργία εσόδων από το δημιουργικό περιεχόμενο χρηστών, πάντα με ασφαλή τρόπο.
3) **Φήμη,** κάθε χρήστης μπορεί να δει τις ενέργειες που πραγματοποιήθηκαν εντός του δικτύου καθώς και να δημιουργήσει ιστορικό κινήσεων.

3.6.2 Bernstein

Σύμφωνα με τους δημιουργούς του, το Bernstein αποτελεί μια εφαρμογή ιστού, από το οποίο κάθε χρήστης του μπορεί με τη βοήθεια της τεχνολογίας του Blockchain να επισημάνει με τη χρήση ψηφιακών ιχνών, περιουσιακά στοιχειά που του ανήκουν. Κάθε χρήστης που κατέχει οποιοδήποτε ψηφιακό περιουσιακό στοιχείο εντός λίγης ώρας μπορεί να το εγγράψει ως δικό του στο δίκτυο. Έπειτα, σε πραγματικό χρόνο τα ανάλογα περιουσιακά στοιχεία, με τη χρήση της παρούσας πλατφόρμας θα μπορούν να αποδείξουν την ύπαρξή τους, τον πραγματικό ιδιοκτήτη τους καθώς και να αναπτυχθούν στο χρόνο.

Η πλατφόρμα διαθέτει διάφορα χαρακτηριστικά. Μερικά από τα οποία είναι, η διατήρηση όλων των έργων κάθε χρήστη σε ένα και μόνο μέρος, μέσα στο οποίο κρυπτογραφούνται τοπικά και με ένα μοναδικό κλειδί τα πάντα. Επιπλέον, συνδυάζει την εμβέλεια που έχει το Blockchain με την αξιοπιστία εθνικών αρχών χρονοσήμανσης (ΕΕ και Κίνα) για τη δημιουργία απόδειξης δικαιωμάτων. Η πλατφόρμα δίνει την δυνατότητα τα πιστοποιητικά να δεθούν μεταξύ τους, και έτσι κάθε χρήστης μπορεί να αποδείξει την πρόοδο του έργου του, κατά την πάροδο του χρόνου. Κάθε ενημερωμένη έκδοση είναι καταχωρημένη στο χρόνο μέσω της εφαρμογής αυτής.

Ωστόσο, το πιο βασικό χαρακτηριστικό της συγκεκριμένης εφαρμογής αποτελεί το ότι όλα τα συμβολαιογραφικά δεδομένα των χρηστών παραμένουν απόλυτα ιδιωτικά και προσβάσιμα μόνο στους κατάλληλους χρήστες, χάρη σε ένα μοναδικό επίπεδο κρυπτογράφησης που χρησιμοποιείται.

4. Προβληματισμοί

Όπως γνωρίζουμε και από τον πραγματικό κόσμο τίποτα δεν μπορεί να θεωρηθεί ως απόλυτο, ιδιαίτερα όταν πρόκειται για μια ανθρώπινη δημιουργία. Αν και πρόκειται για μια ιδέα που φαίνεται πως δίνει πραγματικές λύσεις σε αρκετά από τα προβλήματα της καθημερινότητας, εμπεριέχει μειονεκτήματα ή ακόμη και προκλήσεις. Το βασικότερο αρνητικό που προκύπτει με την χρήση των περισσότερων Blockchain είναι η μεγάλη ηλεκτρική και υπολογιστική ισχύ που χρειάζεται για τη λειτουργεία του ένα τέτοιο δίκτυο. Έχει αναφερθεί ότι στα περισσότερα δίκτυα που υπάρχει η διαδικασία της εξόρυξης, γίνεται μεγάλη κατανάλωση ενέργειας λόγω των αλγορίθμων συναίνεσης που χρησιμοποιούνται. Ωστόσο, είναι αρκετά θετικό πως υπάρχουν νέοι αλγόριθμοι και νέες πλατφόρμες ανάπτυξης που μειώνουν την ανάγκη ενέργειας στο ελάχιστο με τη χρήση διαφορετικών τεχνικών.

Στα επόμενα υποκεφάλαια αναφέρονται κίνδυνοι και προβληματισμοί που προκύπτουν κατά τη χρήση της συγκεκριμένης τεχνολογίας.

4.1 Κυβερνοεπιθέσεις στα Blockchain

Όπως και σε άλλα ψηφιακά συστήματα, πχ το τραπεζικό, επιτήδειοι μπορούν να επιτεθούν και στα Blockchain για την αποκόμιση κάποιου κέρδους. Αν και οι παρακάτω τακτικές είναι σχεδόν αδύνατο να επιτευχθούν, δημόσια δίκτυα που κάνουν χρήση των αλγορίθμων συναίνεσης *PoS* και *PoW* είναι σχετικά πιο ευάλωτα από άλλα που είναι ιδιωτικής χρήσης, χρησιμοποιούν διαφορετικούς αλγορίθμους και τρόπους προστασίας. Αναφέρονται κάποιοι από τους πιο διαδεδομένους τρόπους ψηφιακών επιθέσεων στα δίκτυα Blockchain.

- **Επίθεση *DDos*** (*DDos attack*), ίσως η πιο ευρέως γνωστή τεχνική κυβερνοεπίθεσης, η οποία υπήρχε χρόνια πριν την εμφάνιση του Blockchain και ως στόχο έχει διακομιστές υπηρεσιών. Κατά την επίθεση πολλοί χρήστες δημιουργούν παρόμοια αιτήματα για την απόκτηση δεδομένων προς τον ίδιο διακομιστή. Αυτό έχει ως αποτέλεσμα ο διακομιστής να μην μπορεί να ανταποκριθεί σε όλα τα αιτήματα και να εμφανίζει διάφορα σφάλματα κατά τη λειτουργεία

του . Στα περισσότερα δίκτυα Blockchain υπάρχει προστασία για τις επιθέσεις *DDos*, ωστόσο θεωρητικά υπάρχουν τεχνικές που μπορούν να χρησιμοποιηθούν για την παράκαμψη της παρούσας προστασίας.

- **Επίθεση 51%** (Attack of 51%), γνωστή και ως majority attack, μπορεί να πραγματοποιηθεί οργανωμένα είτε μεμονωμένα, είτε από ένα είτε από σύνολο κόμβων. Ο σκοπός πραγματοποίησης τέτοιας επίθεσης είναι η αναδιοργάνωση της αλυσίδας. Πρόκειται για επίθεση που πραγματοποιείται όταν κάποιος κατέχει τουλάχιστον το 51% της συνολικής υπολογιστικής ισχύος του δικτύου. Από αυτό το σημείο και μετά η κατάσταση για το δίκτυο θεωρείται κρίσιμη έως και επικίνδυνη. Οι κόμβοι που κατέχουν το 51% ξεκινούν να δημιουργούν κρυφά και μεταξύ τους μια αλυσίδα block. Στη συνέχεια, αυτή η αλυσίδα πρόκειται να δημοσιευτεί στο δίκτυο και αυτό θα τροποποιηθεί ριζικά. Απώτερος σκοπός είναι ο ολικός έλεγχος της αλυσίδας για τη δημιουργία μεγάλου ποσοστού κέρδους.
- **Διπλή σπατάλη** (Double-spending), μια διαδικασία κατά την οποία ο ίδιος χρήστης προσπαθεί να χρησιμοποιήσει τα ακριβώς ίδια χρήματα - περιουσιακά στοιχεία για την ταυτόχρονη πραγματοποίηση πολλών συναλλαγών. Η παραπάνω επίθεση γίνεται κυρίως με τη χρήση κρυπτονομισμάτων, καθώς για την πραγματοποίηση συναλλαγών υπάρχει χρονική καθυστέρηση, την οποία επιτήδειοι εκμεταλλεύονται με διάφορους τρόπους για την πραγματοποίηση πολλών παράλληλων συναλλαγών με τα ίδια ακριβώς νομίσματα.
- **Σιβυλλική επίθεση** (Sybil's attack), ένα είδος ψηφιακής επίθεσης όπου ένας χρήστης δημιουργεί πολλούς λογαριασμούς σε μια διαδικτυακή υπηρεσία, για την εκμετάλλευσή της. Στη συγκεκριμένη περίπτωση του Blockchain προσπαθεί ώστε να έχει μεγαλύτερο κέρδος από άλλους χρήστες του δικτύου. Αυτό όμως είναι αδύνατο να γίνει στα δίκτυα με πρωτόκολλο *PoW* καθώς υπάρχει ένα όριο υπολογιστικής δύναμης που μπορεί να παραχθεί από τον υπολογιστή που έχει κάθε χρήστης και για την αύξηση της παραγόμενης ισχύος από κάθε χρήστη, είναι αναγκαία η αγορά επιπλέον συστημάτων, διαδικασία η οποία επιβαρύνει τον χρήστη.
- **Κβαντικοί υπολογιστές**, με την ανάπτυξη των κβαντικών υπολογιστών, συστημάτων με τεράστια υπολογιστική ισχύ, αρκετές φορές πολλαπλάσια από αυτή που έχουν σήμερα οι γνωστοί υπολογιστές. Με τη χρήση κβαντικών αλγορίθμων πχ. Shor, είναι δυνατή η αναστροφή των κρυπτογραφημένων συναρτήσεων κατακερματισμού στην αρχική κατάσταση των δεδομένων, με σκοπό την εύρεση της εισόδου (input) της συνάρτησης. Συγκεκριμένα οι κρυπτογραφικές συναρτήσεις RSA, ECDSA, ECDH και DSA είναι ιδιαίτερα ευάλωτες στην χρήση του αλγορίθμου Shor και γίνονται μη ικανοί για την παροχή προστασίας. Ωστόσο οι κβαντικοί υπολογιστές είναι σε πρώιμο στάδιο ακόμη και η απόκτησή τους είναι αδύνατη να γίνει από απλούς χρήστες, καθώς υπάρχει μεγάλο κόστος απόκτησης. Η κατάσταση με το μεγάλο κόστος εκτιμάτε ότι θα παραμένει για πολλά χρόνια ακόμη. Οι περισσότεροι αλγόριθμοι που χρησιμοποιούνται σε αρκετές από τις υλοποιήσεις Blockchain για τα ζεύγη ασύμμετρων κλειδιών θα πρέπει να αντικατασταθούν στο μέλλον καθώς είναι αρκετά ευάλωτοι απέναντι σε κβαντικούς υπολογισμούς. Στον παρακάτω **πίνακα 3** παρουσιάζονται μερικοί δημοφιλείς και αξιόπιστοι αλγόριθμοι που χρησιμοποιούνται ή έχουν άμεση σχέση με αυτούς

που χρησιμοποιούνται στα Blockchain, καθώς και η επίδραση που έχουν σε αυτούς οι κβαντικοί υπολογιστές.

Πίνακας 3. *Κρυπτογραφικοί αλγόριθμοι και κβαντικοί υπολογιστές*

Κρυπτογραφικός Αλγόριθμος	Τύπος	Βασικός Σκοπός	Επίδραση Κβαντικών υπολογιστών
SHA-2, SHA-3	Μονής Κατεύθυνσης	Κατακερματισμός	Ευπαθής, απαραίτητη η εξέλιξη του
RSA	Δημόσιο κλειδί	Ψηφ. Υπογραφές, σετ κλειδιών	Μη ασφαλής πλέον
ECDSA, ECDH	Δημόσιο κλειδί	Ψηφ. Υπογραφές, σετ κλειδιών	Μη ασφαλής πλέον
DSA	Δημόσιο κλειδί	Ψηφ. Υπογραφές, σετ κλειδιών	Μη ασφαλής πλέον

Ωστόσο καθώς η επέλαση των κβαντικών αποτελεί σημαντικό κίνδυνο για τον γενικότερο κόσμο της κρυπτογραφίας, ήδη από το 2006 ερευνητές εργάζονται πάνω σε έναν τομέα ο οποίος ονομάζεται μετα-κβαντική κρυπτογραφία. Η έρευνα στοχεύει στην επίτευξη μυστικότητας και στον αναπτυγμένο και γρήγορο εντοπισμό περιπτώσεων υποκλοπών. Ειδικότερα από τους τέσσερεις επιμέρους κατηγορίες, εμπεριέχει και έναν, ο οποίος σχετίζεται άμεσα τον κατακερματισμό δεδομένων.

- Κρυπτογραφία βασισμένη στον κατακερματισμό (Hash based cryptography), που αποτελεί και τον βασικό κίνδυνο για την τεχνολογία του Blockchain.

Όπως παρατηρούμε και στον *Πίνακα 3* οι αλγόριθμοι που βασίζονται στην κρυπτογραφία με τη χρήση συμμετρικού κλειδιού ή είναι μονής κατεύθυνσης, δεν κινδυνεύουν άμεσα από τους κβαντικούς υπολογιστές. Με την χρήση μεγαλύτερων στην έξοδο αλφαριθμητικών, φαίνεται ότι θα παραμείνουν το ίδιο ασφαλείς όπως είναι σήμερα και σε μία μετα-κβαντική εποχή.

Οι παραπάνω τακτικές επίθεσης αποτελούν τις πιο ευρέως διαδομένες μορφές κυβερνοεπιθέσεων. Σαφώς το φαινόμενο των κυβερνοεπιθέσεων δεν σταματάει μόνο στις πέντε αυτές περιπτώσεις. Υπάρχουν άτομα που εργάζονται για την ανακάλυψη κενών ασφαλείας και στοχεύουν στη διόρθωσή τους ή στην αποκόμιση κάποιου κέρδους από το κενό αυτό.

Κάποιες από τις εξίσου γνωστές μεθόδους επίθεσης είναι η *Border Gateway Protocol Hijacking, Eclipse Attack, Balance, Block-withholding, DNS Highjacks, Partition Routing, Fork-After-Withhold, Bribery, Pool Reentrancy, Refund, Replay, Selfish mining, Short-address, Finney* κ.α.

Αν και αναφέρθηκαν τρόποι επίθεσης σε Blockchain είναι σημαντικό να σημειωθεί ότι είναι σε θεωρητικό επίπεδο. Στην πραγματικότητα οι περιπτώσεις κυβερνοεπιθέσεων που πραγματοποιήθηκαν είναι ελάχιστες. Οι προκλήσεις που υπάρχουν και θα υπάρχουν, είναι τεράστιες, ωστόσο θα πρέπει να καταβάλλουμε αρκετή προσπάθεια για την ανάπτυξη του

Blockchain και την λύση των προβλημάτων του. Αν και υπάρχουν αρνητικά στη χρήση του, τα οφέλη που λαμβάνουμε τα υπερνικούν.

(Πολυτίδου, 2018)

4.2 Κακόβουλοι χρήστες

Αν και τα Blockchain είναι δίκτυα με κανόνες για τον τρόπο πραγματοποίησης συναλλαγών, σε κάθε χρήστη δεν επιβάλλεται ένας κώδικας συμπεριφοράς ο οποίος να περιορίζει εντός ποιων ορίων μπορεί να κινηθεί.

Το συγκεκριμένο πρόβλημα παρατηρείται στα δημόσιο δίκτυα καθώς μπορεί να συμμετάσχει οποιοσδήποτε και με ουσιαστικά άπειρους λογαριασμούς. Επειδή βασικό χαρακτηριστικό είναι η ανωνυμία, δεν υπάρχει τρόπος να γνωρίζουμε άμεσα ποιος χρήστης βρίσκεται πίσω από κάθε διεύθυνση στο δίκτυο. Αν και αρκετά από τα δημόσια δίκτυα δίνουν κάποια ανταμοιβή στους χρήστες τους ανάλογα με το συνολικό συνεισφερόμενο έργο τους, με στόχο την παρακίνηση τους να λειτουργούν νόμιμα. Επιπλέον υπάρχουν και χρήστες οι οποίοι θα λειτουργήσουν και έκνομα εάν καταλάβουν ότι μπορούν να έχουν μεγαλύτερο κέρδος με συγκεκριμένες τακτικές. Ο τρόπος με τον οποίο οι ίδιοι στοχεύον να βλάψουν το σύστημα είναι η απόκτηση μεγάλης επίδρασης στο δίκτυο, πχ επίθεση 51%. Έπειτα μπορούν να γίνουν οι ακόλουθες πράξεις:

- Απόρριψη συναλλαγών από συγκεκριμένους χρήστες.
- Δημιουργία και στη συνέχεια δημοσίευση μια τροποποιημένης αλυσίδας στο δίκτυο με απώτερο σκοπό τον πλήρη έλεγχό του.
- Απόρριψη της μετάδοσης των block και σε άλλους κόμβους του δικτύου με απώτερο σκοπό τη μη ορθή διανομή πληροφοριών σε όλους τους συμμετέχοντες (η συγκεκριμένη τακτική δεν είναι δυνατή σε αποκεντροποιημένα δίκτυα που διαθέτουν τα κατάλληλα πρωτόκολλα ασφαλείας)

Αξίζει να σημειωθεί ότι πέρα από τους απλούς χρήστες ενός δικτύου, κακόβουλες τακτικές μπορούν να εφαρμοστούν και από τους διαχειριστές του συστήματος. Ωστόσο όλες οι κακόβουλες πράξεις μπορούν να εντοπισθούν και να καταπολεμηθούν άμεσα, με τακτικές hard fork.

4.3 Το ερώτημα των επιχειρήσεων

Πολλές επιχειρήσεις στοχεύουν στην καινοτόμα τεχνολογία και όταν ακούν Blockchain σκέφτονται τρόπους για την εφαρμογή του στις επιχειρήσεις τους. Ωστόσο σε μια νέα τεχνολογία, πολλές επιχειρήσεις έχουν το ερώτημα «Θέλουμε να χρησιμοποιήσουμε το Blockchain, ωστόσο που μπορεί η τεχνολογία αυτή να μας βοηθήσει;».

Τα Blockchain, τουλάχιστον στην παρούσα κατάστασή τους δεν μπορούν να έχουν εφαρμογές σε όλα τα επιχειρησιακά προβλήματα. Για να είναι η σωστή επιλογή θα πρέπει να υπάρχουν οι παρακάτω ανάγκες από την επιχείρηση.

- Μεγάλος αριθμός χρηστών.
- Κατανεμημένοι χρήστες σε πολλά φυσικά σημεία.
- Ανάγκη για την μη ύπαρξη τρίτων (χρηστών ή επιχειρήσεων) που θα συμμετέχουν στην υλοποίηση.
- Η εργασία να βασίζεται σε κάποιου είδους συναλλαγής μεταξύ δύο η περισσοτέρων μερών.
- Ανάγκη για ύπαρξη ενός ασφαλούς και κρυπτογραφημένου συστήματος.
- Ανάγκη για έλεγχο κάθε κίνησης των χρηστών του συστήματος.

4.4 Το ρίσκο της υιοθέτησης

Το Blockchain αποτελεί μια ανερχόμενη και πολλά υποσχόμενη τεχνολογία, η οποία όπως έχει προαναφερθεί, έχει ένα τεράστιο εύρος παροχής λύσεων σε μεγάλο μέρος του επιχειρηματικού κλάδου. Οι περισσότερες από τις υιοθετήσεις Blockchain αποτελούν ριζοσπαστικές καινοτομίες. Όπως συμβαίνει σε κάθε περίπτωση, έτσι και εδώ η υιοθέτηση άκρως καινοτόμων λύσεων ελλοχεύει σημαντικούς κινδύνους για τους εμπλεκόμενους. Εκτός από τα ρίσκα κακόβουλης χρήσης και κυβερνοεπιθέσεων που προαναφέρθηκαν υπάρχουν επιπλέον ρίσκα της υλοποίησης, τα οποία αναλύονται στη συνέχεια.

Αλλαγή της συμπεριφοράς, η αλλαγή είναι σταθερή, ωστόσο στη φύση του ανθρώπου υπάρχει το φαινόμενο της αντίστασης στην αλλαγή. Είναι σίγουρο πως όλες οι επιχειρήσεις και οι φορείς που θα αποφασίσουν τη δημιουργία υπηρεσιών Blockchain είτε άμεσα είτε στο μέλλον για τη βελτιστοποίηση των υπηρεσιών τους, θα περάσουν από αυτή την περίοδο.

Κλιμάκωση, η κλιμάκωση των υπηρεσιών που βασίζονται στο Blockchain αποτελεί μια πρόκληση και ειδικότερα για έναν χρήστη που πρόκειται να χρησιμοποιήσει το Blockchain για πρώτη φορά. Για να εκτελέσει μια απλή συναλλαγή, στην αρχή θα πρέπει να συνδεθεί στο δίκτυο και να κατεβάσει στον δικό του υπολογιστή το καθολικό αρχείο του δικτύου καθώς και να επικυρωθεί αυτό πριν την πραγματοποίηση της συναλλαγής.

Ψηφιοποίηση, η μεταφορά ήδη υπαρχουσών συμβολαίων, επιχειρηματικών εγγράφων και γενικότερα απτών δεδομένων στη νέα μεθοδολογία του Blockchain παρουσιάζει ένα σημαντικό σύνολο εργασιών ψηφιοποίησης που πρέπει να εκτελεστούν. Οι συγκριμένες διαδικασίες ανεξαρτήτως από το ποιος θα είναι ο διάδοχος, χρειάζονται αρκετό χρόνο και μεγάλο κόστος για την υλοποίηση τους.

Κρατικός μηχανισμός και νομολογία, στις συναλλαγές που βασίζονται στο Blockchain, κυβερνητικές υπηρεσίες και υπουργία πιθανών να επιβραδύνουν την ευρεία και ταχεία υιοθέτηση του, με την εισαγωγή νέων νόμων για την συμμόρφωση και τον έλεγχο των εταιρειών που θα παρέχουν τέτοιου είδους υπηρεσίες. Γενικότερα η διαδικασία της συμμόρφωσης είναι χρονοβόρα, ωστόσο εάν τα κράτη θέλουν, μπορούν να επιταχύνουν την διαδικασία. Ήδη παρατηρούμε ότι κράτη εμπιστεύονται τα εργαλεία του Blockchain και προσπαθούν να το φέρουν και στον πραγματικό κόσμο, όπως η Νότια Κορέα που εργάζεται στο να δώσει τη δυνατότητά το bitcoin να χρησιμοποιείται και για τις καθημερινές συναλλαγές των πολιτών της.

5. Συμπεράσματα

Ο αρχικός σκοπός της παρούσας εργασίας ήταν η γενική παρουσίαση του Blockchain και εφαρμογών που χρησιμοποιούνται στην καθημερινότητα. Ωστόσο έγινε μια επιπλέον εμβάθυνση σε αρκετά κύρια αντικείμενα του πυρήνα ενός Blockchain συστήματος, μεταξύ των οποίων, οι μηχανισμοί συναίνεσης, η κρυπτογραφία, γενικά προβλήματα, περιπτώσεις κυβερνοεπιθέσεων καθώς και οι κίνδυνοι που παραμονεύουν με την χρήση του.

Το Blockchain είναι μία καινούρια τεχνολογία που προσφέρει μεγάλη επεκτασιμότητα και ασφάλεια σε πολλούς τομείς, μεταξύ των οποίων οι συναλλαγές, η διακίνηση προϊόντων, ο διαμοιρασμός απόρρητων και μη δεδομένων, χωρίς την ανάγκη ύπαρξης κεντρικής ελεγκτικής αρχής. Από το 2009 που έκανε την πρώτη της εμφάνιση, δίνει συνεχώς λύσεις σε προβλήματα που υπάρχουν στον κόσμο.

Η πρώτη εμφάνιση της τεχνολογίας έγινε με τη δημιουργία και τη δημοσίευση ενός ψηφιακού νομίσματος, το οποίο ήταν το πρώτο που παρείχε ένα καθολικό αρχείο συναλλαγών το οποίο διαμοιραζόταν μεταξύ όλων των χρηστών του. Για λόγους ασφαλείας, αποφασίστηκε να μην υπάρχει σύνδεση των προσώπων με στοιχεία που μπορούν να χρησιμοποιούν στον πραγματικό κόσμο, για τη διασφάλιση της ανωνυμίας. Επιπλέον λειτουργείες για την κρυπτογράφηση της ψηφιακής ταυτότητας των χρηστών χρησιμοποιήθηκαν. Το καθολικό αρχείο, καταγράφει με ασφάλεια κάθε είδους κίνηση που πραγματοποιείται στο δίκτυο. Για την ορθή λειτουργεία των δικτύων κάθε φορά που προσπαθεί μια συναλλαγή να εκτελεστεί, γίνεται έλεγχος στο αρχείο ότι πρόκειται για συναλλαγή που μπορεί να πραγματοποιηθεί.

Η τεχνολογία του Blockchain βρίσκεται ακόμη στα πρωταρχικά της στάδια, αλλά αποτελεί έναν βαθιά ερευνημένο τομέα. Την παρούσα χρονική στιγμή υπάρχει μεγάλη προώθηση της συγκεκριμένης τεχνολογίας καθώς και των λύσεων που η την χρήση της μπορεί να επιφέρει στον κόσμο γενικά. Είναι σίγουρο ότι στο μέλλον με την ευρεία ανάπτυξη, το Blockchain θα αποτελεί ένα ακόμη βασικό εργαλείο που θα χρησιμοποιεί ο ψηφιακός κόσμος.

Όπως αναφέρθηκε σε αυτή την πτυχιακή εργασία, το Blockchain κάνει χρήσεις σε τεχνολογίες δικτύων, συναλλαγών, κρυπτογράφησης και διατήρησης αρχείων, αλλά για πρώτη φορά βλέπουμε τους παραπάνω τομείς να συνδυάζονται τόσο αρμονικά και να παρέχουν ένα πολύ καλό αποτέλεσμα. Θα είναι πολύ σημαντικό οι οργανισμοί να ξεκινήσουν να ελέγχουν εάν οι λύσεις των Blockchain τους συμφέρουν καθώς τα πλεονεκτήματα της τεχνολογίας αυτής υπερνικούν τα ελάχιστα μειονεκτήματα που έχει. Ωστόσο η παραπάνω διαδικασία θα πρέπει να γίνεται σχολαστικά και με πλήρη ανάλυση ώστε να αποφευχθούν λάθη, τα οποία μετά για να επιλυθούν θα είναι δύσκολα και μεγάλα σε κόστος.

Το βασικό χαρακτηριστικό αμεταβλητότητας των δεδομένων θα παίξει σημαντικό ρόλο στην επιλογή από οργανισμούς, καθώς όλοι οι οργανισμοί για λόγους ιστορικότητας και ασφάλειας θέλουν να διατηρούν τα διάφορα αρχεία τους όσο πιο ολοκληρωμένα γίνεται. Ωστόσο, τουλάχιστον στις ημέρες μας το Blockchain δεν μπορεί να παρέχει λύσεις σε όλα τα είδη των επιχειρήσεων. Με την πάροδο του χρόνου θα βλέπουμε περισσότερες λειτουργίες να προστίθενται και περισσότερες επιχειρήσεις να κάνουν εφαρμογή κάποιας τέτοιας λύσης.

Λόγω του τεράστιου ενδιαφέροντος που υπάρχει για την τεχνολογία, συνεχώς δημιουργούνται start-up εταιρείες που προσπαθούν να φέρουν κάτι καινοτόμο στον τομέα. Σύμφωνα με εκτιμήσεις αυτές οι εταιρείες, όπως και με τις περισσότερες start-up, πρόκειται να μην έχουν ένα αισιόδοξο μέλλον μιας και λίγες από αυτές θα καταφέρουν να δημιουργήσουν την υλοποίηση που θα τους φέρει στην κορυφή. Η υιοθέτηση μιας τέτοιας λύσης αποτελεί μεγάλη πρόκληση για τις εταιρείες που πρόκειται να το χρησιμοποιούν στο μέλλον.

Ωστόσο, εταιρείες κολοσσοί και ειδικότερα στον χρηματοοικονομικό τομέα μεταξύ των οποίων παροχή χρεωστικών/πιστωτικών καρτών και χρηματιστηριακοί δείκτες κάνουν ήδη χρήση κάποιου είδους λύσεων Blockchain και επενδύουν μεγάλα ποσά για την ανάπτυξη ολοκληρωμένων εφαρμογών. ΄

Τέλος, αυτό που πραγματικά συμβαίνει από πολλούς είναι ότι δεν προσπαθούν μόνο να βελτιώσουν την απόδοση και αξιοπιστία των εφαρμογών τους, σκοπεύουν και στη αναζήτηση νέων επιχειρηματικών μοντέλων, με την χρήση των οποίων θα μπορούσαν να έχουν και κάποιο κέρδος στο άμεσο ή έμμεσο μέλλον. Εκτιμάτε ότι στις επόμενες 1-2 δεκαετίες θα δούμε ένα σημαντικά αυξημένο ποσοστό καινοτόμων εφαρμογών για την αξιοποίηση της Blockchain τεχνολογίας.

Βιβλιογραφία

Alharby, M. a. (2017, Αύγουστος). Blockchain Based Smart Contracts : A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*, σσ. 125– 140. doi:10.5121/csit.2017.71011

Andrew, P. (2020, August 28). *What is Proof of Capacity? An Eco-Friendly Mining Solution.* Ανάκτηση από Coincentral: https://coincentral.com/what-is-proof-of-capacity/

Bano, S., & al., e. (2017, Νοέμβριος 14). *arXiv:1711.03936v2.* Ανάκτηση από Consensus in the Age of Blockchains: https://arxiv.org/abs/1711.03936

BigchainDB GmbH, Berlin, Germany. (2018, Μάιος). *BigchainDB 2.0The Blockchain Database.* Ανάκτηση Ιούλιος 20, 2020, από BigchainDB: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Binance Academy. (χ.χ.). *Delegated Proof of Stake Explained*. Ανάκτηση Αύγουστος 28, 2020, από Binance Academy: https://academy.binance.com/blockchain/delegated-proof-of-stake-explained

Binance.academy. (χ.χ.). *Hards Forks and Soft Forks Explained*. Ανάκτηση Αύγουστος 12, 2020, από Binance.academy: https://academy.binance.com/en/articles/hard-forks-and-soft-forks

binance.charity. (χ.χ.). *Blockchain Charity Foundation - Binance.charity*. Ανάκτηση Αύγουστος 20, 2020, από Binance.charity: https://www.binance.charity/about

Brilliant. (2020, 31 Αύγουστος). *Merkle Tree*. Ανάκτηση από Brilliant Math & Science Wiki: https://brilliant.org/wiki/merkle-tree/

DHL. (2020, Σεπτέμβριος 20). *DHL Global*. Ανάκτηση από Blockchain: https://www.dhl.com/global-en/home/insights-and-innovation/insights/blockchain.html

EOS.IO. (2018, Μάιος). *Documentation/TechnicalWhitePaper.* Ανάκτηση Ιούνιος 19, 2020, από EOS.IO Technical White Paper v2: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

Ethereum. (n.d.). *What is ethereum?* Ανάκτηση Ιούλιος 15, 2020, από Ethereum.org: https://ethereum.org/en/what-is-ethereum/

Frankenfeld, J. (2020, Αύγουστος 29). *Proof of Elapsed Time (PoET)*. (S. Anderson, Επιμελητής) Ανάκτηση Σεπτέμβριος 9, 2020, από Investopedia: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

Haber, S., & Stornetta, W. (1991, January). How to time-stamp a digital document. *J. Cryptology*(3), σσ. 99-111. doi:https://doi.org/10.1007/BF00196791

Hedera. (χ.χ). *Hedera Hashgraph*. Ανάκτηση Αύγουστος 28, 2020, από Hedera Hashgraph: https://www.hedera.com/

Hyperledger - Sawtooth. (χ.χ.). *Introduction - Sawtooth v1.0.5 Documentation*. Ανάκτηση Αύγουστος 5, 2020, από Sawtooth: https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html

Hyperledger. (2018). *Hyperledger Architecture, Volume II Smart Contracts.* Ανάκτηση Ιούλιος 16, 2020, από Hyperledger: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

Infopulse. (2019, Οκτώβριος). *Blockchain in Supply Chain Management: Key Use Cases and Benefits.* Ανάκτηση Σεπτέμβριος 11, 2020, από Medium: https://medium.com/@infopulseglobal_9037/blockchain-in-supply-chain-management-key-use-cases-and-benefits-6c6b7fd43094

Jayachandran, P. (2017, Μάιος 31). *The difference between public and private blockchain*. Ανάκτηση Ιούνιος 4, 2020, από IBM Blogs: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Kouklas, N. (2018). *Overview, Challenges and Applications of Blockchain Technologies.* Patras.

Leslie, L. (1998). The Part-Time Parliament. *ACM Transactions on Computer Systems, 16*(2), 133-169.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing List*, 1-9. Ανάκτηση Ιούνος 2, 2020, από https://bitcoin.org/bitcoin.pdf

Nodes. (n.d.). *Blockchain Nodes: An In-Depth Guide*. Ανάκτηση Ιούλιος 15, 2020, από Nodes: https://nodes.com/

OpenChain. (n.d.). *Overview of Openchain*. Ανάκτηση Αύγουστος 19, 2020, από OpenChain Documentation: https://docs.openchain.org/en/latest/general/overview.html

OpenLaw. (χ.χ.). *OpenLaw Documentation*. Ανάκτηση Ιούνιος 30, 2020, από OpenLaw: docs.openlaw.io

Pilkington, M. (2016). Blockchain technology: principles and applications. Στο *Research Handbook on Digital Transformations* (σσ. 225–253).

Quorum. (2018). *Quorum Whitepaper.* Ανάκτηση από https://github.com/ConsenSys/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf

R3. (n.d.). *Blockchain/DLT 101*. Ανάκτηση Ιούνιος 4, 2020, από R3: https://www.r3.com/blockchain-101/

R3. (n.d.). *Enterprise Blockchain Platform*. Ανάκτηση από R3: https://www.r3.com/corda-platform/

Robinson, K. (2018, Σεπτέμβριος 21). *What is Public Key Cryptography?* Ανάκτηση Αύγουστος 16, 2020, από Twilio: https://www.twilio.com/blog/what-is-public-key-cryptography

Sarmah, S. S. (2018, Αύγουστος 02). *Understanding Blockchain Technology.* doi:10.5923/j.computer.20180802.02

Treum. (χ.χ.). *Treum*. Ανάκτηση Σεπτέμβριος 28, 2020, από Treum: https://treum.io/

Unibright.io. (2017, Δεκέμβριος 7). *Blockchain evolution: from 1.0 to 4.0.* Ανάκτηση Ιούνιος 7, 2020, από Medium: https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666

What is BitHope. (χ.χ.). Ανάκτηση Σεπτέμβριος 5, 2020, από Bithope: https://bithope.org/what-is-bithope

XRP. (χ.χ.). Ανάκτηση Αύγουστος 29, 2020, από Ripple: https://ripple.com/xrp/

Yaga, D., & al., e. (2018, October). *NISTIR 8202.* National Institute of Standards and Technology. doi:10.6028/nist.ir.8202

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, (σσ. 557-564). Honolulu, HI. doi:10.1109/BigDataCongress.2017.85

Μπεκρή, Ε. (2020). *Σύγκριση Τεχνολογιών Κατανεμημένης Εγγραφής "Blockchain".* Διπλωματική Εργασία, ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ, ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, Αθήνα. Ανάκτηση Ιούλιος 29, 2020, από http://artemis.cslab.ece.ntua.gr:8080/jspui/handle/123456789/17663

Πολυτίδου, Ε. (2018). *Τεχνολογίες Blockchain σε Συστήματα Υποδομής Δημόσιου.* Πτυχιακή Εργασία , Ελληνικό Ανοικτό Πανεπιστήμιο, Σχολή Θετικών Επιστημών και Τεχνολογίας, Πάτρα. Ανάκτηση Ιούλιος 29, 2020, από https://apothesis.eap.gr/handle/repo/37470