ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Το Blockchain, τα κρυπτονομίσματα και πως θα αλλάξει για πάντα ο τρόπος πληρωμών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΛΑΙΟΛΟΓΟΥ ΜΙΧΑΗΛ

2016

Επιβλέπων : Βέργαδος Δημήτριος

Ιδιότητα

Καστοριά Μήνας - Έτος (παρουσίασης της εργασίας)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Το Blockchain, τα κρυπτονομίσματα και πως θα αλλάξει για πάντα ο τρόπος πληρωμών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΛΑΙΟΛΟΓΟΥ ΜΙΧΑΗΛ

(ΑΕΜ: 2016)

Επιβλέπων : Βέργαδος Δημήτριος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

....

Καστοριά Μήνας - Έτος (παρουσίασης της εργασίας

ΠΕΡΙΛΗΨΗ

Η παρακάτω πτυχιακή εργασία θα μας αναλύσει σε λεπτομερή επίπεδα τα κρυπτονομίσματα, το δίκτυο που τα στηρίζει καθώς και τις μεθόδους που οι επενδυτές εξορίσουν τα κρυπτονομίσματα τους. Θα δούμε πως δημιουργήθηκαν, τον δημιουργό τους και την αντίδραση της κοινωνίας πάνω τους καθώς θα προσπαθήσουμε να καταλάβουμε που οδεύουν και το γιατί το μέλλον του διαδικτύου βασίζεται άμεσα μαζί τους.

Στα παρακάτω κεφάλαια θα αναλυθεί επίσης και το Blockchain λεπτομερώς όπως και τα σταθερά σε αξία κρυπτονομίσματα και πως πετυχαίνουν να έχουν την σταθερή τιμή του ενός δολαρίου. Θα δούμε τα επίπεδα του διαδικτύου και το μέλλον του και τελικώς θα δούμε τους κινδύνους που κρύβουν για τα αφελή άτομα. Τέλος θα πραγματοποιηθεί μια βασική ανάλυση σε όσα έχουμε δει και θα πούμε τα συμπεράσματα που πάρθηκαν.

Λέξεις κλειδιά: Κρυπτονόμισμα, Blockchain, NFT, DAO, DEX, Stablecoin, Ethereum, Bitcoin, Binance, Proof of Work, Proof of Stake, Proof of History, Proof of Burn, Hard Fork, Soft Fork, Hot Wallet, Cold Wallet, DeFi

Summary

In the following thesis will analyze in detailed levels the cryptocurrency, the network that supports it, as well as the methods that the investors use to mine their cryptocurrency. We will take a look on how they were created, their creator and the reaction society had on them and we will try to understand their future and why the future of the internet is based directly on them.

In the following chapter, Blockchain will be analyzed in detail as well as the stable in value, Stablecoins and how they manage to keep their price stable at one dollar. We will see the levels of the Web and its future and finally we will take a look at the dangers the unsuspected people can get on. Finally, a basic analysis will be made of what we have seen and we will say the conclusions that we reached.

Key Words: Cryptocurrency, Blockchain, NFT, DAO, DEX, Stablecoin, Ethereum, Bitcoin, Binance, Proof of Work, Proof of Stake, Proof of History, Proof of Burn, Hard Fork, Soft Fork, Hot Wallet, Cold Wallet, DeFi

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Λίστα εικόνων 9
1. ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ BLOCKCHAIN 10
1.1. Τι είναι τα κρυπτονομίσματα 10
1.2. Τι είναι το Blockchain 11
1.2.1. Ιστορία του Blockchain 13
1.2.2. Περιπτώσεις χρήσης του Blockchain σήμερα 15
1.2.3. Περιπτώσεις χρήσης του Blockchain στο παρόν και στο μέλλον 19
2. ΟΙ ΔΥΟ ΓΙΓΑΝΤΕΣ ΚΑΙ ΤΑ ΣΤΑΘΕΡΑ ΝΟΜΙΣΜΑΤΑ 25
2.1. Bitcoin και Ethereum 25
2.2. Ethereum 27
2.2.1. NFT 29
2.3. Stablecoins 32
2.3.1. Ασφαλισμένα stablecoins 33
2.3.2. Μη ασφαλισμένα stablecoins 34
2.3.3. Ρυθμισμένα stablecoins 34
2.4. Decentralized Autonomous Organization (DAO) 35
3. ΧΡΗΣΙΜΟΤΗΤΑ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ 37
3.1. Εξόρυξη 37
3.1.1. Proof of Work 40
3.1.2. Proof of Stake 44
3.1.3. Proof of History 46
3.1.4. Proof of Burn 47
3.2. HARD FORKS/SOFT FORKS 50
3.3. Κινητά πορτοφόλια 52
3.3.1. Ψηφιακό πορτοφόλι 53
3.4. DeFi 55
3.4.1. Πλατφόρμες δανεισμού 59
3.4.2. Stablecoins 60
3.4.3. Αγορές πρόβλεψης 60
3.5. Stock market/Crypto market 60

3.6. Centralization/Decentralization 63
3.6.1. Decentralized Exchange 64
4. Η ΕΞΕΛΙΞΗ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ 66
4.1. Web1.0 66
4.2. Web 2.0 66
4.3. Web 3.0 68
5. Metaverse 71
5.1. Κίνδυνοι 74
5.1.1. Τα κρυπτονομίσματα ως ιδιοκτησία 75
5.1.2. Η κατάσταση της αποκέντρωσης 76
5.1.3. Επιχειρήσεις και αδειοδότηση 77
5.3.4. Ξέπλυμα χρήματος 77
6. ΣΥΜΠΕΡΑΣΜΑΤΑ 78
ΒΙΒΛΙΟΓΡΑΦΙΑ 78

Λίστα εικόνων

Εικόνα 1: Τα πέντε πιο δημοφιλές κρυπτονομίσματα της χρονιάς 2021 11
Εικόνα 2: Παράδειγμα δημιουργίας ενός block στο δίκτυο του bitcoin 13
Εικόνα 3: Smart contract γραμμένο στην γλώσσα Solidity 17
Εικόνα 4: Ο δημιουργός του ethereum εξηγεί με δικά του λόγια το ethereum στο Disrupt SF 29
Εικόνα 5: Τα διάσημα Cryptokitties NFT 32
Εικόνα 6: Τα 3 πιο δημοφιλή stablecoins (από πάνω): DAI, USD Coin, Tether 35
Εικόνα 7: Διάγραμμα παραδείγματος Proof of Work(PoW) 43
Εικόνα 8: Διάγραμμα παραδείγματος Proof of Stake(PoS) 46
Εικόνα 9: Παράδειγμα διαγράμματος των Fork από την σελίδα Investopedia 51
Εικόνα 10: Διαφορές μεταξύ hot(αριστερά) και cold(δεξιά) wallet 55
Εικόνα 11: Διαφορές των Web1.0, Web 2.0, Web 3.0 71
Εικόνα 12: Ο διευθύνον σύμβουλος του Facebook δημιουργεί το δικό του avatar στο metaverse του Meta 74

1. ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ BLOCKCHAIN

1.1. Τι είναι τα κρυπτονομίσματα

Ένα κρυπτονόμισμα είναι ένα ψηφιακό ή εικονικό νόμισμα ασφαλισμένο με κρυπτογραφία, γεγονός που το καθιστά σχεδόν αδύνατον να παραβιαστεί ή να χρησιμοποιηθεί περισσότερες φορές από όσες θα έπρεπε. Πολλά κρυπτονομίσματα είναι αποκεντρωμένα δίκτυα που βασίζονται στην τεχνολογία blockchain. Ένα καθοριστικό χαρακτηριστικό των κρυπτονομισμάτων είναι ότι γενικά δεν εκδίδονται από καμία κεντρική αρχή, γεγονός που θεωρητικά τα καθιστά απρόσβλητα σε κρατικές παρεμβάσεις ή χειραγωγήσεις.

Τα κρυπτονομίσματα είναι συστήματα που επιτρέπουν ασφαλείς πληρωμές στο διαδίκτυο, οι οποίες εκφράζονται με εικονικά tokens, τα οποία αντιπροσωπεύονται από εγγραφές στο εσωτερικό του συστήματος. Το "κρύπτο" στην λέξη κρυπτονόμισμα αναφέρεται στους διάφορους αλγόριθμους κρυπτογράφησης και στις κρυπτογραφικές τεχνικές που προστατεύουν τις εγγραφές, όπως είναι η κρυπτογράφηση ελλειπτικής καμπύλης, τα ζεύγη δημόσιου-ιδιωτικού κλειδιού και οι συναρτήσεις κατακερματισμού.

Το πρώτο κρυπτονόμισμα που βασίστηκε στο blockchain ήταν το Bitcoin, το οποίο εξακολουθεί να παραμένει το πιο δημοφιλές και το πιο πολύτιμο. Σήμερα, υπάρχουν χιλιάδες εναλλακτικά κρυπτονομίσματα με διάφορες λειτουργίες και προδιαγραφές. Μερικά από αυτά είναι κλώνοι του Bitcoin, ενώ άλλα είναι νέα νομίσματα που δημιουργήθηκαν από την αρχή.

Τα κρυπτονομίσματα χρησιμοποιούν συνήθως έναν αποκεντρωμένο έλεγχο σε αντίθεση με τα ψηφιακά νομίσματα της κεντρικής τράπεζας. Όταν ένα κρυπτονόμισμα δημιουργείται πριν από την έκδοση ή εκδίδεται από κάποιον εκδότη, θεωρείται γενικά ότι μπορεί να ελεγχθεί. Όταν εφαρμόζεται με αποκεντρωμένο έλεγχο, κάθε κρυπτονόμισμα λειτουργεί μέσω της τεχνολογίας του κατανεμημένου καθολικού του, συνήθως με ένα blockchain, που χρησιμεύει ως βάση δεδομένων για τις δημόσιες οικονομικές συναλλαγές.

Κεντρικό στοιχείο για την λειτουργικότητα του Bitcoin και άλλων κρυπτονομισμάτων είναι η τεχνολογία blockchain, η οποία χρησιμοποιείται για τη διατήρηση ενός διαδικτυακού καθολικού από όλες τις συναλλαγές που έχουν πραγματοποιηθεί ποτέ, παρέχοντας έτσι μια δομή δεδομένων στο συγκεκριμένο καθολικό, που είναι αρκετά ασφαλής και είναι κοινόχρηστο σε ολόκληρο το δίκτυο ενός μεμονωμένου κόμβου ή υπολογιστή που διατηρεί ένα αντίγραφο του. Κάθε νέο μπλοκ που δημιουργείται πρέπει να επαληθεύεται από κάθε κόμβο πριν επιβεβαιωθεί, καθιστώντας σχεδόν αδύνατη τη πλαστογράφηση ιστορικών συναλλαγών.

Το πιο δημοφιλές κρυπτονόμισμα, το bitcoin, έχει ασταθείς κινήσεις τιμών, φτάνοντας σχεδόν τα 65.000 δολάρια τον Απρίλιο του 2021 πριν χάσει σχεδόν τη μισή αξία του τον Μάιο. Μέχρι τα μέσα Νοεμβρίου, η τιμή είχε αυξηθεί ξανά γρήγορα: έφτασε στην πιο υψηλή τιμή του κοντά στα 70.000 δολάρια πριν υποχωρήσει. [5, 6, 7, 10]

Εικόνα 1: Τα πέντε πιο δημοφιλές κρυπτονομίσματα της χρονιάς 2021[33]

1.2. Τι είναι το Blockchain

Ένα Blockchain είναι μια νέα τεχνολογία οι οποία παρουσιάζεται ως μια δημόσια, μη δυνάμενη να τροποποιηθεί ως προς το ιστορικό της διανεμημένη σειρά δεδομένων, ομαδοποιημένων σε χρονικά αριθμημένα *τμήματα*, *συστοιχίες* (*μπλοκ*). Με πιο απλά λόγια, το Blockchain είναι μια λίστα με μπλοκ που συνδέονται αλυσιδωτά μεταξύ τους μέσω ενός κρυπτογραφικού κατακερματισμού(*hash*).

Το δημόσιο βιβλίο κρυπτονομισμάτων είναι ένα σύστημα τήρησης αρχείων. Το βιβλίο διατηρεί τις ταυτότητες των συμμετεχόντων ανώνυμες, το ποσό που έχουν διαθέσιμο σε κρυπτονομίσματα και ένα αρχείο όλων των αυθεντικών συναλλαγών που εκτελούνται μεταξύ των συμμετεχόντων στο δίκτυο.

Ένα μπλοκ καταγράφει ορισμένες ή όλες τις πιο πρόσφατες συναλλαγές που δεν έχουν ακόμη καταχωριστεί σε κανένα προηγούμενο μπλοκ. Έτσι, ένα μπλοκ είναι σαν μια σελίδα ενός βιβλίου. Κάθε φορά που ένα μπλοκ «ολοκληρώνεται», δίνει τη θέση του στο επόμενο μπλοκ στο Blockchain. Ένα μπλοκ είναι επομένως μια μόνιμη αποθήκευση εγγραφών που, αφού γραφτούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν.

Το κάθε μπλοκ περιέχει πληροφορίες για το παρελθόν του και το μέλλον του. Μόλις ολοκληρωθεί ένα μπλοκ, αποτελεί κομμάτι τού παρελθόντος του και ‘κάνει’ χώρο για ένα καινούργιο μπλοκ στην λίστα τού Blockchain. Το ολοκληρωμένο μπλοκ αποτελεί μέρος μιας συναλλαγής που έγινε στο παρελθόν και οι καινούργιες πληροφορίες καταγράφονται στο νέο μπλοκ.

Με αυτόν τον τρόπο το συνολικό σύστημα λειτουργεί κυκλικά και η πληροφορία παραμένει καταγεγραμμένη στο Blockchain. Κάθε μπλοκ περιλαμβάνει εγγραφές ορισμένων ή όλων των πρόσφατων συναλλαγών μαζί με μια αναφορά στο μπλοκ που προηγήθηκε, το οποίο, μαζί με το σύστημα επαλήθευσης peer-to-peer του Blockchain, καθιστά σχεδόν αδύνατο για έναν χρήστη να παραβιάσει τα δεδομένα συναλλαγών που είχαν καταγραφεί προηγουμένως. Κάθε ένα μπλοκ περιέχει μέσα του έναν header καθώς και ένα body.

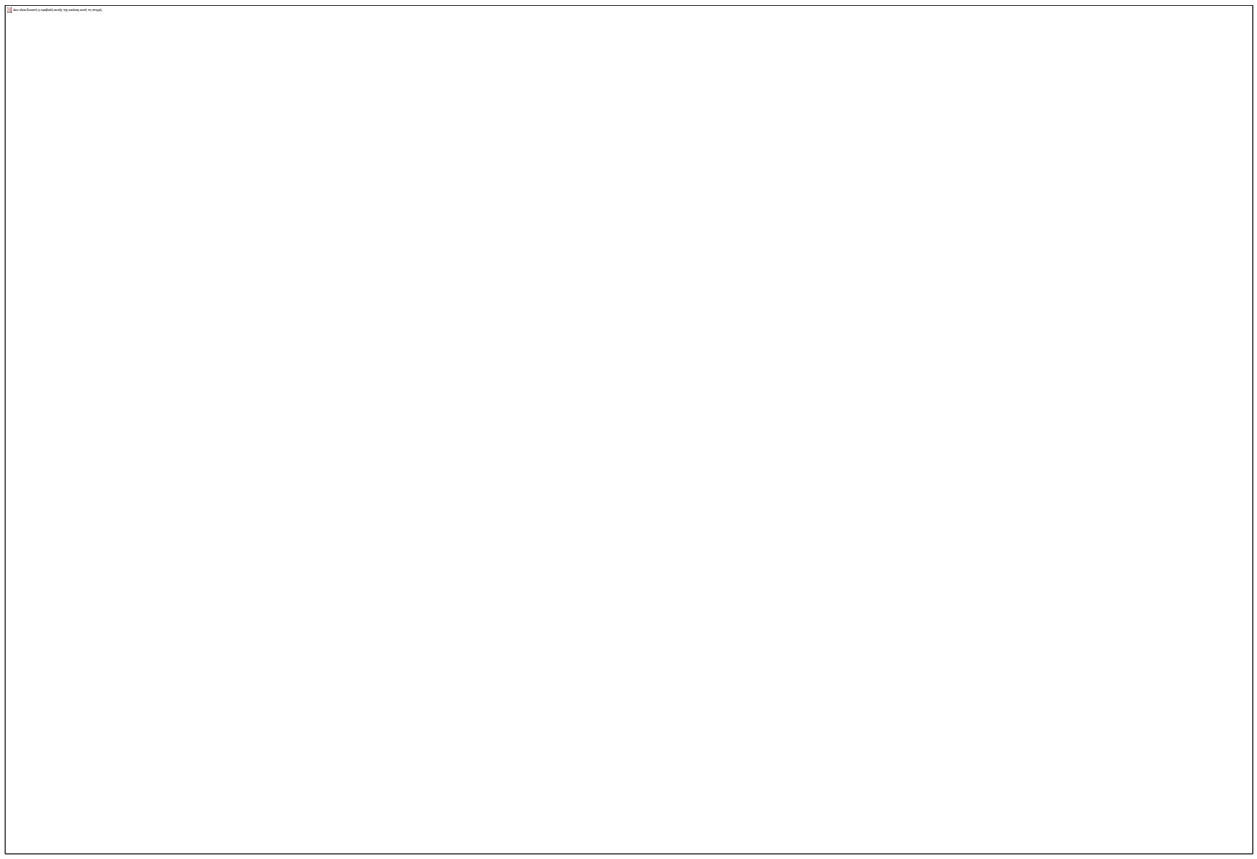
Το header αποτελείται από 6 μέρη: τον αριθμό έκδοσής του, τον κρυπτογραφικό κατακερματισμό του προηγούμενου στην σειρά μπλοκ, τον κατακερματισμό ρίζας του δέντρου Merkle, ο χρόνος σε δευτερόλεπτα από της 01-01-1970 00:00 UTC, ο στόχος της τρέχουσας δυσκολίας και το nonce.

Ο αριθμός έκδοσης δεν έχει ιδιαίτερη σημασία, ωστόσο κάποιος που κάνει εξορύξεις(*mining*), μπορεί να υποδείξει ποιες αποφάσεις τού πρωτοκόλλου υποστηρίζει αν έχει έναν συγκεκριμένο αριθμό έκδοσης. Ο κρυπτογραφικός κατακερματισμός τού προηγούμενου μπλοκ είναι ο τρόπος που συνδέονται τα μπλοκ αλυσιδωτά. Επειδή ο κρυπτογραφικός κατακερματισμός τού προηγούμενου μπλοκ περιέχεται στον κατακερματισμό τού νέου μπλοκ, τα μπλοκ τού blockchain στηρίζονται το ένα πάνω στο άλλο. Χωρίς αυτό το στοιχείο, δεν θα υπήρχε σύνδεση και χρονολογία μεταξύ του κάθε μπλοκ.

Όλες οι συναλλαγές που περιέχονται σε ένα μπλοκ μπορούν να συγκεντρωθούν σε έναν κρυπτογραφικό κατακερματισμό. Αυτός είναι και ο ριζικός κρυπτογραφικός κατακερματισμός του δέντρου Merkle. Ο χρόνος σε δευτερόλεπτα από της 01-01-1970 UTC είναι η χρονική σήμανση η οποία είναι βασικός παράγοντας για την παραγωγή του κρυπτογραφικού κατακερματισμού στο μπλοκ.

Ο στόχος της τρέχουσας δυσκολίας υποδεικνύει πόσο μικρός πρέπει να είναι ο νέος κρυπτογραφικός κατακερματισμός για να είναι έγκυρος. Με άλλα λόγια, κάθε κατακερματισμός έχει ένα μέγεθος σε bit. Όσο χαμηλότερος είναι ο στόχος σε bit, τόσο πιο δύσκολο είναι να βρεθεί ένας αντίστοιχος κατακερματισμός. Ένας κατακερματισμός με πολλά μηδενικά στην αρχή είναι μικρότερος από έναν κατακερματισμό χωρίς μηδενικά.

Το nonce είναι η μεταβλητή που προσαυξάνεται με την μέθοδο “απόδειξη εργασίας”(*proof of work*). Με αυτόν τον τρόπο, ο εξορύκτης(*miner*) μαντεύει έναν έγκυρο κρυπτογραφικό κατακερματισμό, έναν κατακερματισμό που είναι μικρότερος από τον στόχο. Το πρώτο μπλοκ σε μια αλυσίδα από μπλοκ ονομάζεται genesis.[1, 5]



Εικόνα 2: Παράδειγμα δημιουργίας ενός block στο δίκτυο του bitcoin[32]

1.2.1. Ιστορία του Blockchain

1982: Ο κρυπτογράφος David Chaum πρότεινε για πρώτη φορά ένα πρωτόκολλο παρόμοιο με το blockchain στην διατριβή του "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups".

1991: Μια κρυπτογραφικά ασφαλής αλυσίδα από μπλοκ περιγράφεται για πρώτη φορά από τους Stuart Haber και W Scott Stornetta.

1992: Το 1992, οι Haber, Stornetta και Dave Bayer ενσωμάτωσαν τα δέντρα Merkle στο σχέδιο τους, τα οποία βελτίωσαν την αποτελεσματικότητά του επιτρέποντας τη συλλογή πολλών πιστοποιητικών εγγράφων από ένα μπλοκ(*smart contracts*).

1995: Μέσα από την εταιρεία τους, Surety, τα κατακερματισμένα πιστοποιητικά εγγράφων τους(*hashes*) δημοσιεύονται στους New York Times κάθε εβδομάδα από το 1995.

1998: Ο επιστήμονας υπολογιστών Nick Szabo εργάζεται στο «bit gold», ένα αποκεντρωμένο ψηφιακό νόμισμα.

2000: Ο Stefan Konst δημοσίευσε τη θεωρία του για κρυπτογραφικές ασφαλείς αλυσίδες, καθώς και ιδέες για την εφαρμογή τους.

2008: Στα τέλη τού 2008 δημοσιεύθηκε ένα “έγγραφο με πληροφορίες”(*white paper*) από ένα άτομο ή μια ομάδα, αυτοαποκαλούμενη Satoshi Nakamoto. Ο/οι Nakamoto βελτίωσε σημαντικά τον σχεδιασμό χρησιμοποιώντας μια μέθοδο παρόμοια με την Hashcash έτσι ώστε να σηματοδοτήσει χρονικά τα μπλοκ χωρίς να χρειάζεται να είναι υπογεγραμμένα από έμπιστα μέλη και παρουσίασε μια μέθοδο δυσκολίας για να ισοσταθμίσει τον ρυθμό που μπαίνουν τα μπλοκ στην αλυσίδα.

2009: Το πρώτο bitcoin μπλοκ εξήχθη από τον Satoshi Nakamoto και είχε ως αμοιβή 50 bitcoin. Ο Nakamoto εφαρμόζει το πρώτο blockchain ως ένα δημόσιο μέσο συναλλαγής για συναλλαγές που πραγματοποιούνται με την χρήση τού bitcoin. Ο πρώτος αποδέκτης τού Bitcoin ήταν ο Hal Finney, ο οποίος έλαβε 10 bitcoins από τον Satoshi Nakamoto στην πρώτη συναλλαγή bitcoin στον κόσμο στις 12 Ιανουαρίου 2009.

2013: Ο Vitalik Buterin, Ρώσος προγραμματιστής και συνιδρυτής του περιοδικού Bitcoin Magazine, δήλωσε ότι το Bitcoin χρειαζόταν μια γλώσσα γραφής για τη δημιουργία αποκεντρωμένων εφαρμογών, τα λεγόμενα decentralized applications.

Όταν δεν δέχτηκαν την πρόταση του, ο Vitalik ξεκίνησε την ανάπτυξη μιας νέας πλατφόρμας κατανεμημένων υπολογιστών βασισμένων στο blockchain, το Ethereum, που περιλάμβανε μια λειτουργικότητα scripting, γνωστή και ως έξυπνο συμβόλαιο(smart contract). Τα έξυπνα συμβόλαια γράφονται σε συγκεκριμένες γλώσσες προγραμματισμού και μεταγλωττίζονται σε bytecode, την οποία μπορεί να διαβάσει και να εκτελέσει μια αποκεντρωμένη εικονική μηχανή Turing-complete, που ονομάζεται εικονική μηχανή Ethereum (EVM).

2014-2020: Τον Αύγουστο τού 2014 το μέγεθος τού bitcoin Blockchain έφτασε σε μέγεθος τα 20 GB περιέχοντας μέσα του όλες τις συναλλαγές που έγιναν στο δίκτυο. Τον Ιανουάριο τού 2015, το μέγεθος αυξήθηκε σχεδόν 30 GB και από τον Ιανουάριο τού 2016 μέχρι τον Ιανουάριο τού 2017, το μέγεθος αυξήθηκε από 50 GB σε 100 GB αντίστοιχα. Το 2020 το μέγεθος των συναλλαγών είχε φτάσει τα 200 GB.

Η πρώτη ιστορικά εφαρμογή της τεχνολογίας blockchain ήταν το ψηφιακό νόμισμα Bitcoin, του Satoshi Nakamoto. Στην εργασία αυτή προτεινόταν μια λύση σε ένα διάσημο πρόβλημα των Μαθηματικών με εφαρμογή της λύσης αυτής στον χρηματοοικονομικό τομέα.

Ήταν δυνατόν η ανθρώπινη κοινωνία να χτίσει ένα δίκτυο από υπολογιστές και μέσω του δικτύου αυτού να εκτελούν χρηματοοικονομικές συναλλαγές μεταξύ τους με μαθηματικός αποδεδειγμένης ασφάλειας και διαφύλαξης των περιουσιών τους και ταυτόχρονα να μην υπάρχει μια κεντρική εξουσία που να μπορεί να αλλάζει με οποιοδήποτε τρόπο θα ήθελε, τους κανονισμούς, οι οποίοι διέπουν την πραγματοποίηση ή όχι όλων αυτών των συναλλαγών.

Οι κανονισμοί αυτοί σχεδιάστηκαν από τον προγραμματιστή του Πρωτοκόλλου αυτού και αποτελούν το Πρωτόκολλο Συναίνεσης του Bitcoin, το οποίο χρησιμοποιεί έναν αλγόριθμο

απόδειξης μόχθου. Σήμερα χρησιμοποιούνται και άλλοι αλγόριθμοι, όπως ο αλγόριθμος απόδειξης μερισμάτων στο ψηφιακό νόμισμα Ethereum.

Σύμφωνα με την Accenture, μια εφαρμογή της θεωρίας της διάχυσης των καινοτομιών, υποδηλώνει ότι το Blockchain χρησιμοποιείτε στο 13.5% στις χρηματοοικονομικές υπηρεσίες του 2016, φτάνοντας επομένως στη φάση της πρώιμης υιοθέτησης. Οι βιομηχανικοί εμπορικοί όμιλοι δημιούργησαν το Παγκόσμιο Φόρουμ Blockchain το 2016, μια πρωτοβουλία του Chamber of Digital Commerce.

2018-2019: Τον Μάιο του 2018, ο Gartner διαπίστωσε ότι μόνο το 1% των CIO(chief information office) ανέφεραν οποιοδήποτε είδος υιοθέτησης blockchain στους οργανισμούς τους και μόνο το 8% των CIO ήταν είχαν βραχυπρόθεσμο «σχεδιασμό ενεργού πειραματισμού με το blockchain». Για το έτος 2019 ο Gartner ανέφερε ότι μόνο το 5% των CIO πίστευαν ότι η τεχνολογία blockchain ήταν μια «αλλαγή» για την επιχείρησή τους.

Ο χρόνος μπλοκ(*block time*) είναι ο μέσος χρόνος που χρειάζεται για να δημιουργήσει το δίκτυο ένα επιπλέον μπλοκ στην αλυσίδα. Ορισμένες αλυσίδες μπλοκ δημιουργούν ένα νέο μπλοκ τόσο συχνά όσο κάθε πέντε δευτερόλεπτα. Μέχρι τη στιγμή της ολοκλήρωσης του μπλοκ, τα δεδομένα που περιλαμβάνονται καθίστανται επαληθεύσιμα στα κρυπτονομίσματα.

Αυτό είναι πρακτικά όταν πραγματοποιείται μια συναλλαγή, επομένως ένας μικρότερος χρόνος αποκλεισμού σημαίνει ταχύτερες συναλλαγές. Ο χρόνος αποκλεισμού για το Ethereum έχει οριστεί μεταξύ 14 και 15 δευτερολέπτων, ενώ για το bitcoin είναι κατά μέσο όρο 10 λεπτά.[1, 2, 4, 5]

1.2.2. Περιπτώσεις χρήσης του Blockchain σήμερα

Αν και ακόμα η τεχνολογία του Blockchain απέχει πολύ από μια ώριμη τεχνολογία, το Blockchain κατέχει μια εξέχουσα θέση ως μια υγιής και εξαιρετικά ασφαλής μέθοδος συναλλαγών σε πολλαπλές βιομηχανίες και εφαρμογές.

Η τεχνολογία του Blockchain είναι μια δημόσια βάση δεδομένων που παρακολουθεί τις συναλλαγές που γίνονται στο δίκτυό της. Οι συναλλαγές, περιλαμβάνονται σε ένα μπλοκ το οποίο δεν μπορεί να αλλαχθεί ποτέ και με κανένα τρόπο. Κάθε ένα μπλοκ, έχει μια χρονοσφραγίδα, και ενώνεται με το προηγούμενο μπλοκ, καθώς και με το επόμενο μόλις εκείνο γεμίσει, έτσι ώστε να δημιουργηθεί μια αλυσίδα.

Η πιο συχνή χρησιμότητά του είναι ως ένα κατανεμημένο καθολικό, όπου όλοι οι χρήστες του συμφωνούν στην εγκυρότητά του και πιστοποιούν τις συναλλαγές προτού δημιουργηθεί το μπλοκ μέσα στο Blockchain, καθώς και υπάρχουν ορισμένα ιδιωτικά Blockchain με λίγους ή κανέναν συμμετέχοντα.

Σύμφωνα με μια έρευνα του Forrester Consulting Blockchain του 2019 που ανατέθηκε από την EY(παλαιότερα γνωστή ως Ernst & Young), ο Chen Zur, US Blockchain practice leader της EY είπε “η διατήρηση της ακεραιότητας των δεδομένων ήταν ο νούμερο ένας λόγος και ο

πιο συχνός, για την δημιουργία και διατήρηση του Blockchain. Περίπου οι μισοί από τους ερωτηθέντες, δήλωσαν ότι θα προτιμούσαν οι χρησιμότητες του Blockchain, να βελτίωναν το ίδιο το Blockchain και να ενσωμάτωναν και άλλες επιλογές, όπως τα διαθέσιμα προϊόντα και ο εντοπισμός τους, η υποστήριξη των πληρωμών και η ψηφιοποίηση των ροών των εγγράφων".

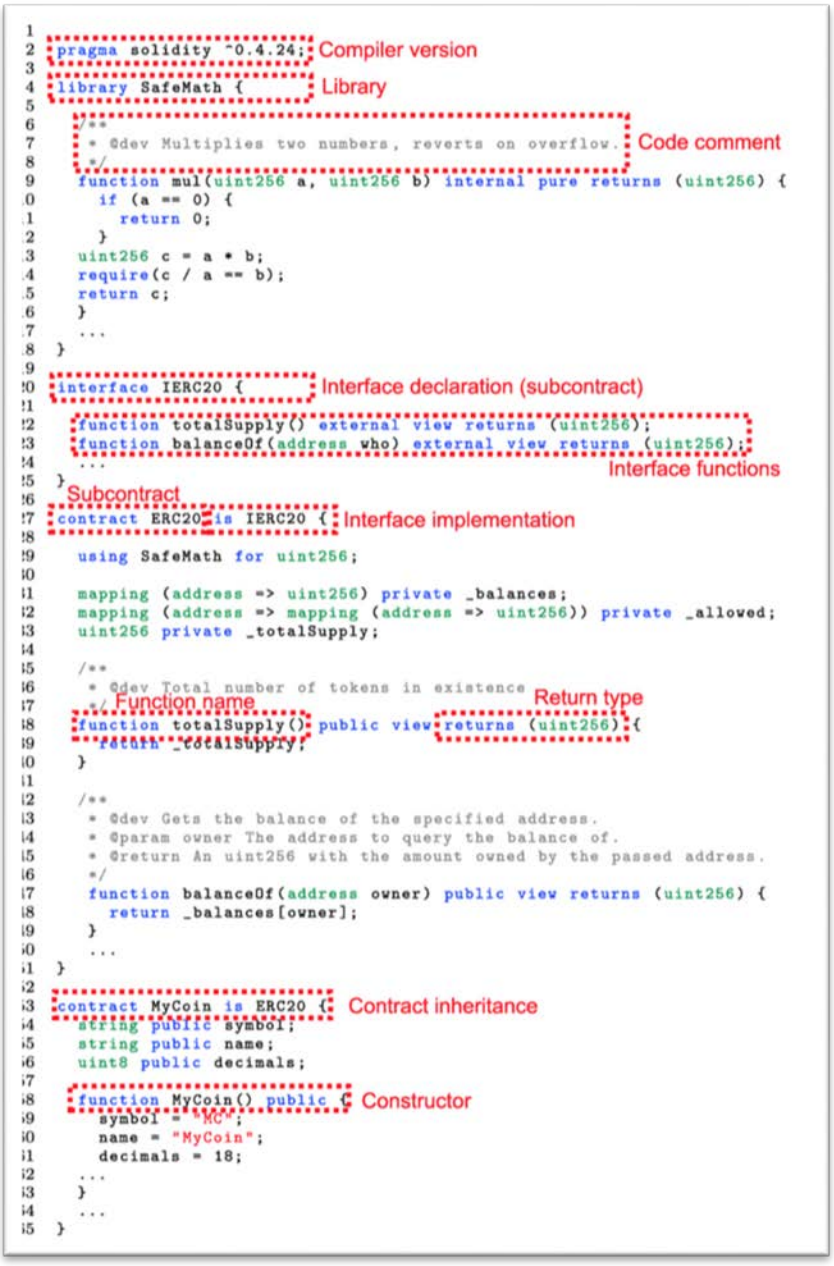
Ο Jitin Agarwal, που είναι αντιπρόεδρος μηχανικής στην εταιρεία 84.51˚, δήλωσε πως "Οι περιπτώσεις χρήσης του Blockchain προς το παρόν, δεν είναι γενικές, αλλά φορούν εταιρείες, βιομηχανίες και λειτουργείες. Οι οργανισμοί θα πρέπει να ψάξουν στις δραστηριότητές τους, για να καταλάβουν, ποια από τα πέντε βασικά οφέλη του Blockchain(διαφάνεια, διακυβέρνηση, ασφάλεια, δημόσια πρόσβαση ή αμετάβλητο/έλεγχος), είναι το πιο πολύτιμο".

Το Blockchain είναι «μια τεχνολογία γενικής χρήσης, που σημαίνει ότι είναι εφαρμόσιμη σε όλους τους τομείς», δήλωσε ο Χρήστος Μακρίδης, ερευνητικός καθηγητής στο Πολιτειακό Πανεπιστήμιο της Αριζόνα, ανώτερος σύμβουλος στο Gallup, ψηφιακός συνεργάτης στο Εργαστήριο Ψηφιακής Οικονομίας του Πανεπιστημίου Στάνφορντ και CTO στην τεχνολογία των τεχνών και της εκπαίδευσης startup Living Opera. "Για παράδειγμα, οι χρηματοπιστωτικές υπηρεσίες μπορούν να το χρησιμοποιήσουν για τη σύνταξη έξυπνων συμβάσεων μεταξύ των καταναλωτών και του τραπεζικού τους ιδρύματος. Ομοίως, η υγειονομική περίθαλψη μπορεί να το χρησιμοποιήσει για τη σύνταξη έξυπνων συμβολαίων μεταξύ ασφαλιστών και νοσοκομείων, καθώς και μεταξύ ασθενών και νοσοκομείων. Οι δυνατότητες είναι ατελείωτες."

Οι χρήσεις του Blockchain αυτήν την στιγμή, είναι οι εξής: τα έξυπνα συμβόλαια, η κυβερνοασφάλεια, το internet of things(IOT), τα κρυπτονομίσματα και τα non fungible tokens(NFT).

Στα έξυπνα συμβόλαια αναφερθήκαμε και νωρίτερα αλλά η κύρια χρησιμότητά τους είναι η αυτοματοποίηση των συμβολαίων πριν λήξουν. Ο κώδικάς τους είναι σχετικά απλός και είναι της μορφής "when/if…then…" για να διασφαλίσει πως όλα τα μέλη, λαμβάνουν τα προνόμια ή τα ποινικά ρήτρα όπως ορίζει και το συμβόλαιο. Τα έξυπνα συμβόλαια είναι χρήσιμα και χρησιμοποιούνται από τις περισσότερες βιομηχανίες σήμερα για μια ποικιλία χρήσεων που παραδοσιακά διέπονται με συμβάσεις χαρτιού.

Ακολουθεί ένα απλό παράδειγμα ενός smart contract γραμμένο σε γλώσσα Solidity για το δίκτυο του Ethereum:



Εικόνα 3: Smart contract γραμμένο στην γλώσσα Solidity[34]

Τα Blockchain έχουν ύψιστη ασφάλεια λόγο της μονιμότητας τους, της διαφάνειάς τους και της κατανεμημένη φύση τους. Με τον αποθηκευτικό χώρο του Blockchain, δεν υπάρχει κάποια κεντρική οντότητα για να δεχθεί επίθεση ούτε κάποια κεντρική βάση δεδομένων που θα μπορούσε να παραβιαστεί. Επειδή τα Blockchain είναι αποκεντρωμένα, συμπεριλαμβανομένου και των ιδιωτικών Blockchain, και επειδή τα δεδομένα που αποθηκεύονται σε κάθε μπλοκ δεν μπορούν να αλλαχθούν, καμία εγκληματική οργάνωση δεν θα μπορούσε να αποσπάσει κάποια πληροφορία. “Στην τελική, οι εισβολείς θα χρειάζονται

πολλά διαφορετικά κλειδιά αντί για ένα. Οι υπολογιστικές απαιτήσεις για τον εισβολέα αυξάνονται ραγδαία" ανέφερε ο Χρήστος Μακρίδης.

Οι δύο κύριες χρήσεις IOT του Blockchain, είναι στον τομέα της εφοδιαστικής αλυσίδας για την παρακολούθηση περιουσιακών στοιχείων και της διαχείρισης αποθεμάτων. Μια τρίτη χρήση είναι η καταγραφή των μετρήσεων των μηχανών, είτε αυτοί οι αισθητήρες βρίσκονται στην Αρκτική, είτε στην ζούγκλα του Αμαζονίου, είτε είναι σε κάποιο εργοστάσιο παραγωγής, είτε είναι σε ένα drone της NASA πάνω στον Άρη. "Είτε είναι αναφορές για χημικά δεδομένα περί ποιότητας λαδιού ή για την παρακολούθηση φορτίων ηλεκτρονικών συσκευών παγκόσμια μέσω διαφόρων θυρών εισόδου, το Blockchain μπορεί να χρησιμοποιηθεί οπουδήποτε υπάρχουν δεδομένα που αλληλοεπιδρούν έξω κόσμο" εξήγησε ο Aaron Rafferty, CEO της επενδυτικής εταιρείας R.F. Capital.

Η ιδέα του Blockchain αναπτύχθηκε αρχικά για την διαχείριση ψηφιακών νομισμάτων όπως το bitcoin. Ενώ οι δύο τεχνολογίες εξακολουθούν να ανταγωνίζονται για εναλλακτικές συναλλαγές, έχουν επίσης διαχωριστεί, ώστε τα Blockchain να μπορούν να εξυπηρετούν και άλλους σκοπούς. Δεδομένης της ανωνυμίας των κρυπτονομισμάτων, το Blockchain είναι ο μοναδικός τρόπος καταγραφής των συναλλαγών τους με ασφάλεια και ακρίβεια για τα εμπλεκόμενα μέρη.

Τα non fungible tokens(NFTs) είναι μονάδες δεδομένων, πιστοποιημένα ότι είναι μοναδικά και μη ανταλλάξιμα. Εν ολίγης είναι ψηφιακά περιουσιακά στοιχεία. Θα τα αναλύσουμε περισσότερο στην συνέχεια. Σύμφωνα με τον Rafferty, τα NFTs φέρνουν την επανάσταση στον κόσμο της ψηφιακής τέχνης και των συλλογών παγκοσμίως. "Χρησιμοποιώντας το αποκεντρωμένο Blockchain του ethereum μπορούμε να δημιουργήσουμε ένα δίκτυο με ζωντανή ροή μουσικής όπου οι καλλιτέχνες όπου οι καλλιτέχνες και οι streamers έχουν την δυνατότητα να συνδεθούν με τους θαυμαστές τους απευθείας, να πουλήσουν NFTs, να λάβουν εισφορές από θαυμαστές και να ανταλλάξουν τις αμοιβές τους για κρυπτονομίσματα" είπε ο Shantal Anderson, ιδρυτής και CEO του δικτύου της μουσικής Reel Mood.

"Οι περισσότερες εταιρείες μπορούν να χρησιμοποιήσουν το Blockchain," είπε ο Agarwal της 84.51˚, "αλλά οι εφαρμογές που προσφέρουν τα μεγαλύτερα έσοδα για την εταιρεία, βασίζονται στην βελτιστοποίηση και στην μείωση της τριβής που σχετίζεται με τις συμμετοχές σε κανονικές επιχειρηματικές πρακτικές".

Το να τρέχεις μια επιχείρηση πιο αποτελεσματικά είναι μόνο ένα μέρος των πλεονεκτημάτων που μπορούν να αποκομιστούν από τις εφαρμογές του Blockchain. "Ειδικότερα, η ανάγκη της διατήρησης της ακεραιότητας των δεδομένων και η δυνατότητα δημιουργίας νέων εισόδων ή επιχειρηματικών μοντέλων είναι τα μεγαλύτερα κίνητρα για περισσότερους από τους μισούς ερωτηθέντες", είπε ο Rajat Kapur, senior manager της EY, blockchain practice.[22]

1.2.3. Περιπτώσεις χρήσης του Blockchain στο παρόν και στο μέλλον

Η τεχνολογία του Blockchain έχει διανύσει σημαντικά βήματα στην ανάπτυξη και στην ευρεία υιοθέτησή της τα τελευταία χρόνια, χωρίς να δείχνει κάποιο ίχνος καθυστέρησης. Σύμφωνα με την παγκόσμια έρευνα της Deloitte το 2021 όσον αφορά το Blockchain, σχεδόν το 76% των στελεχών που συμμετείχαν στην έρευνα δήλωσαν ότι περιμένουν τα ψηφιακά περιουσιακά στοιχεία να είναι στο μέλλον μια εναλλακτική των χρημάτων της παγκόσμιας χρηματοδότησης τα επόμενα 5-10 χρόνια.

Αυτό σημαίνει ότι έχει έρθει η στιγμή για την εξέλιξη της επανάστασης πάνω στον τομέα της οικονομίας και της κοινωνίας και θα αλλάξει ο τρόπος με τον οποίο επεξεργαζόμαστε τις συναλλαγές, που διαχειριζόμαστε τα δεδομένα και που παρέχουμε υπηρεσίες.

Δυστυχώς, η τεχνολογία του Blockchain δεν είναι ακόμα ευρέος κατανοητή. Την γνωρίζουμε μόνο ως την τεχνολογία πίσω από τα κρυπτονομίσματα όπως το bitcoin, αλλά αυτό απέχει πολύ από την εφαρμογή του και πολλοί άνθρωποι, δεν συνειδητοποιούν πως η τεχνολογία του Blockchain μπορεί να βοηθήσει τους ίδιους, την εταιρεία τους και την κοινωνία ως σύνολο. Οπότε στην συνέχεια θα δούμε πως θα μοιάζει η τεχνολογία του Blockchain στο μέλλον και τι αλλαγές μπορεί να φέρει.

Οι δυνατότητες της τεχνολογίας του Blockchain είναι πραγματικά ατελείωτες και οι εξελίξεις τα τελευταία χρόνια, μας οδήγησαν ένα βήμα πιο κοντά στην αποκέντρωση, σε ένα αναξιόπιστο διαδίκτυο, στην διαφάνεια των συναλλαγών, και σε πολλά άλλα.

“Φαίνεται ότι το Blockchain ήρθε για να μείνει, νομίζω ότι θα είναι μια ισχυρή τεχνολογία για την σύγχρονη κοινωνία”, είπε ο Reid Hoffman, συνιδρυτής και εκτελεστικός πρόεδρος της εταιρείας LinkedIn. Μερικοί τρόποι που το Blockchain μπορεί να επηρεάσει το μέλλον είναι οι παρακάτω. [23]

1.2.3.1. Non fungible tokens (NFTs)

Στον συνεχώς εξελισσόμενο κόσμο, μια από τις πιο σχετικές περιπτώσεις χρήσης του Blockchain αυτή την στιγμή, είναι τα κρυπτονομίσματα και θα παραμείνουν εδώ τουλάχιστον στο άμεσο μέλλον. Παρόλα αυτά, ένα πιο συναρπαστικό μέλλον που αναδεικνύεται από την τεχνολογία του Blockchain, είναι τα non fungible tokens (NFTs).

Τα NFTs είναι ένας επαναστατικός νέος τρόπος αγοράς και πώλησης ψηφιακών περιουσιακών στοιχείων που αναπαριστούν αντικείμενα του έξω κόσμου. Όλα τα NFTs είναι μοναδικά και δεν μπορούν να αντικατασταθούν, μπορούν μόνο να αγοραστούν, να πωληθούν, να ανταλλαχθούν ή να δοθούν από τον κάτοχο ή τον δημιουργό τους.

Τα NFT θα μπορούσαν να τροφοδοτήσουν ένα εντελώς νέο κύμα ψηφιακών συλλεκτικών ειδών, από σπάνια έργα τέχνης έως μοναδικά αθλητικά παπούτσια και αξεσουάρ.

Θα μπορούσαν επίσης να χρησιμοποιηθούν στην θέση αντικειμένων σε βιντεοπαιχνίδια ή άλλους εικονικούς κόσμους.

Το έτος 2021 θεωρείται το “έτος των NFTs”. Σε μόλις δύο μήνες, σημειώθηκαν σχεδόν 400 εκατομμύρια δολάρια σε ακαθάριστες πωλήσεις για τα δέκα κορυφαία συλλεκτικά αντικείμενα, τα οποία είναι όλα συλλεκτικά αντικείμενα βασισμένα σε κρυπτονομίσματα, σημειώνοντας συνολική αύξηση 400% σε σχέση με τα νούμερα του περασμένου μήνα!

Οι δυνατότητες για τα NFT είναι ατελείωτες — και αυτά τα tokens πιθανότατα θα έχουν σημαντικό αντίκτυπο στο μέλλον της ψηφιακής ιδιοκτησίας. Επιπλέον, τα επόμενα χρόνια, πιθανότατα θα μπορούν να πωληθούν τα πάντα, από έργα τέχνης μέχρι αυτοκίνητα χρησιμοποιώντας NFT. [23, 12]

1.2.3.2. Γρηγορότερες συναλλαγές

Λόγω της ασφαλούς και αποκεντρωμένης φύσης της τεχνολογίας του blockchain, είναι απίστευτα δύσκολο (αν όχι αδύνατο) για τους χάκερ ή κακόβουλες ομάδες να παραβιάσουν τις συναλλαγές. Τα δεδομένα που επαληθεύονται από το Blockchain είναι εξαιρετικά ασφαλή και αξιόπιστα, πράγμα που σημαίνει ότι οι συναλλαγές μπορούν να υποβληθούν σε επεξεργασία πολύ πιο γρήγορα από ό,τι στον σημερινό κόσμο, χωρίς να τίθεται σε κίνδυνο η ασφάλεια.

Ο κλάδος των τραπεζικών και χρηματοοικονομικών υπηρεσιών έχει πάρει μια εντελώς ψηφιακή κατεύθυνση. Έχει προβλεφθεί ότι η τεχνολογία blockchain θα γνωρίσει μια ώθηση στη δημοτικότητα μεταξύ των επαγγελματιών του χρηματοοικονομικού τομέα, με το 66% των τραπεζών να αναμένει να έχουν λύσεις χρησιμοποιώντας το blockchain στην παραγωγή τους μέσα στα επόμενα τρία χρόνια.

Επιπλέον, το μέλλον του blockchain στα χρηματοοικονομικά μας φέρνει επίσης ευκαιρίες να διεκπεραιώσουμε συναλλαγές κάθε μέρα. Χωρίς να διακόπτεται από τις ώρες λειτουργίας της τράπεζας, η τεχνολογία θα μπορούσε να επιτρέψει στις επιχειρήσεις, τις κυβερνήσεις και τους καταναλωτές να πραγματοποιούν συναλλαγές οποτεδήποτε και οπουδήποτε. [23]

1.2.3.3.Ψηφιακή ταυτότητα

Σήμερα, χρησιμοποιούμε κωδικούς πρόσβασης και ερωτήσεις ελέγχου ταυτότητας για να αποδείξουμε ποιοι είμαστε στο διαδίκτυο. Το Blockchain θα μπορούσε να αντικαταστήσει αυτό το σύστημα με μια ψηφιακή ταυτότητα που είναι ασφαλής και εύκολη στη διαχείριση.

Αντί να πρέπει να αποδείξει ο χρήστης ποιος είναι ανακαλώντας κάποια προσωπική, αυθαίρετη πληροφορία που θα μπορούσε ενδεχομένως να μαντέψει ή να κλαπεί, η ψηφιακή του ταυτότητα θα βασίζεται σε ένα μοναδικά τυχαίο σύνολο αριθμών που εκχωρείται για κάθε χρήστη σε ένα δίκτυο blockchain.

Αυτό σημαίνει ότι η ταυτότητά οποιουδήποτε δεν μπορεί να παραβιαστεί ή να αλλάξει χωρίς πρόσβαση στο ιδιωτικό του κλειδί, γεγονός που το καθιστά εκθετικά πιο αξιόπιστο από την τρέχουσα λύση μας. Στην πραγματικότητα, το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας (NIST) ήδη ερευνά πώς το blockchain μπορεί να βοηθήσει στην προστασία των ψηφιακών ταυτοτήτων. [23]

1.2.3.4. Η αγοραπωλησία ακινήτων

Η απόδειξη και η επαλήθευση ταυτότητας έχει γίνει ένα από τα πιο σημαντικά ζητήματα στην ακίνητη περιουσία. Αυτήν τη στιγμή, χρειάζονται μέρες για να ολοκληρώσει μια τράπεζα τη διαδικασία ώστε να μάθει περισσότερα στοιχεία για έναν αγοραστή που κλείνει ένα σπίτι.

Δεδομένου ότι το blockchain καθιστά τα δεδομένα πιο εύκολα ανιχνεύσιμα, αυτή η μακρά διαδικασία επαλήθευσης θα μπορούσε να εξαλειφθεί μέσω των έξυπνων συμβολαίων. Αυτές οι αυτοεκτελούμενες συμβάσεις θα μπορούσαν να συνταχθούν για την εκτέλεση μιας μεγάλης ποικιλίας εργασιών, συμπεριλαμβανομένης της επεξεργασίας αιτημάτων δανείου και της επαλήθευσης ταυτότητας. [23]

1.2.3.5. Προβλήματα υγείας

Όπως αναφέραμε προηγουμένως, οι ψηφιακές ταυτότητες θα μπορούσαν να αποθηκεύονται και να διαχειρίζονται μέσω της τεχνολογίας blockchain — και αυτό ισχύει και για τα αρχεία υγείας.

Οι πάροχοι υγειονομικής περίθαλψης θα μπορούσαν επίσης να χρησιμοποιούν τεχνολογία blockchain για να ανταλλάσσουν δεδομένα μεταξύ τους με ασφάλεια. Αυτό θα μείωνε τις απολύσεις και θα βελτίωνε την ταχύτητα της διάγνωσης, ενώ παράλληλα θα προστατεύει το απόρρητο των ασθενών ανά πάσα στιγμή.

Οι δυνατότητες δεν σταματούν εκεί – το blockchain θα μπορούσε ακόμη και να χρησιμοποιηθεί για την παρακολούθηση της εφοδιαστικής αλυσίδας, τη βελτίωση της ασφάλειας των φαρμάκων και την καταπολέμηση των πλαστών φαρμάκων, τη μείωση των ασφαλίστρων ασφάλισης υγείας και πολλά άλλα.

Επιπλέον, το μέγεθος της παγκόσμιας αγοράς της τεχνολογίας blockchain στην υγειονομική περίθαλψη αναμένεται να φτάσει τα 231 εκατομμύρια δολάρια των ηνωμένων πολιτειών έως το 2022, με ρυθμό ανάπτυξης 63% για τα επόμενα έξι χρόνια (2019-2028). [23]

1.2.3.6. Διευκόλυνση στις ψηφοφορίες

Η ψηφοφορία με την τεχνολογία του Blockchain θα μπορούσε να είναι ευκολότερη, ταχύτερη και πιο ασφαλής από τον τρόπο που ψηφίζουμε σήμερα. Θα βοηθούσε επίσης στην προστασία της ταυτότητας των ψηφοφόρων (ακόμη και στην υποστήριξη της ψηφοφορίας εξ αποστάσεως). Αντί να χρειάζεται να πάνε οι ψηφοφόροι στις κάλπες ή να στείλουν ένα ψηφοδέλτιο μέσω ταχυδρομείου, θα μπορούν απλώς να συνδεθούν στον υπολογιστή ή στην κινητή συσκευή τους, να επαληθεύσουν την ταυτότητά τους και να ψηφίσουν.

Το πιο σημαντικό είναι ότι το Blockchain τα καθιστά όλα αυτά δυνατά, ενώ παρέχει επίσης ένα αμετάβλητο αρχείο ψήφων για την αποτροπή ζητημάτων απάτης ή παραποίησης. Υπάρχουν ήδη πολλές νεοσύστατες εταιρείες blockchain που επικεντρώνονται στο να βοηθήσουν τους ανθρώπους να ψηφίζουν με μεγαλύτερη ασφάλεια στο διαδίκτυο, επομένως μπορεί να μην αργήσει πολύ μέχρι να γίνει η ψηφοφορία μέσω Διαδικτύου κανόνας σε όλο τον κόσμο. [23]

1.2.3.7. Υιοθέτηση κρυπτονομισμάτων

Δεν υπάρχει αμφιβολία ότι τα επόμενα χρόνια, θα μπορούσε να υπάρξει σημαντική αύξηση στην υιοθέτηση κρυπτονομισμάτων. Αυτό θα οδηγούσε σε μια πιο ευρεία χρήση της τεχνολογίας blockchain καθώς οι επιχειρήσεις, τόσο μεγάλες όσο και μικρές, αρχίζουν να δέχονται πληρωμές με κρυπτονομίσματα.

Μέχρι και σήμερα είναι δύσκολο για τους καθημερινούς καταναλωτές να ασχοληθούν με τις συναλλαγές κρυπτονομισμάτων. Αυτό αναμένεται να αλλάξει καθώς εμφανίζονται περισσότερα κρυπτονομίσματα και σιγά σιγά διευκολύνει η χρήση ψηφιακών νομισμάτων όπως το Bitcoin ή το Ethereum.

Αυτό, θα μπορούσε επίσης να οδηγήσει σε ευρεία αξιοποίηση περιουσιακών στοιχείων όπως αυτοκίνητα, σπίτια, γη, έργα τέχνης ή οτιδήποτε έχει αξία. [23]

1.2.3.8. Αγορές αυτοκινήτων χωρίς χρήματα

Η αυτοκινητοβιομηχανία βρίσκεται στη μέση μιας σημαντικής στροφής από την αγορά αυτοκινήτων στον απλό δανεισμό τους. Στο μέλλον, θα γίνεται να πληρωθεί κάποιο όχημα με κρυπτονομίσματα και να πραγματοποιηθεί η πληρωμή του μέσω tokens. Επιπλέον, δεν θα χρειάζεται να υπάρχει ανησυχία για μηνιαίες πληρωμές ή για την ασφάλεια, απλώς θα υπάρχει η δυνατότητα της λήψης μιας εφαρμογής και αφού επιλεχθεί το μοντέλο και η τοποθεσία παραλαβής ο χρήστης θα είναι έτοιμος να ξεκινήσει.

Εν ολίγης, ολόκληρη η διαδικασία θα μπορεί να ολοκληρωθεί μέσα σε λίγα λεπτά. Δεν θα χρειάζεται καν ο πελάτης να επικοινωνήσει με τον πωλητή ή να εγκριθεί από τον έμπορο, θα είναι τα πάντα αυτοματοποιημένα και θα εξαρτώνται από τα κρυπτονομίσματα που θα έχει ο αγοραστής στην κατοχή του.

Όπως φαίνεται, υπάρχουν άπειρες δυνατότητες για την τεχνολογία του Blockchain, οι οποίες συνεχώς αυξάνονται. Το μέλλον της τεχνολογίας του Blockchain φαίνεται λαμπρό και αν σκεφτούμε ότι είναι πολλά υποσχόμενο σε κάθε κλάδο, φαίνεται ότι τα καλύτερα δεν έχουν έρθει ακόμα. [23]

1.2.3.9. Εφοδιασμός

Ένα από τα καλύτερα παραδείγματα όπου η τεχνολογία του Blockchain αξιοποιείται πλήρως, είναι στον τομέα του εφοδιασμού. Όλες οι λειτουργίες στο κομμάτι του εφοδιασμού, θα δουν μια επανάσταση με την άφιξη της τεχνολογίας του Blockchain. Ήδη υπάρχουν τεράστιες εταιρείες που έχουν αρχίσει να χρησιμοποιούν αυτήν την καινούργια τεχνολογία στο κομμάτι του εφοδιασμού.

Ο παγκόσμιος κολοσσός IBM έχει συνεργαστεί με την Maersk, η οποία είναι η μεγαλύτερη εταιρεία στον πλανήτη, που εκμεταλλεύεται τις μεταφορές εμπορευματοκιβωτίων. Με αυτήν την σχέση, ο κολοσσός της τεχνολογίας και ο γίγαντας της βιομηχανίας της εφοδιαστικής αλυσίδας, έχουν ενωθεί για να διευκολύνουν το παγκόσμιο εμπόριο μέσω της τεχνολογίας του Blockchain. Το δίκτυο διανομής, το οποίο εξαπλώνεται παγκοσμίως, αναμένεται να εμφανίσει καλύτερο συντονισμό από το ένα σημείο στο άλλο.

Με τον παραδοσιακό τρόπο λειτουργίας, οι επικοινωνίες θα μπορούσαν εύκολα να προκαλέσουν σύγχυση λόγο του υπερφορτωμένου δικτύου με τα πολλαπλά εμπλεκόμενα μέρη παγκοσμίως. Χρησιμοποιώντας το Blockchain ως λύση, παρομοίως με τις εταιρείες IBM και Maersk, οι εταιρείες αποστολών θα μπορούν να εκτελούν ένα αμετάβλητο σύστημα. Κάθε συναλλαγή θα προστίθεται στο σύστημα το οποίο θα διανέμετε σε ολόκληρη την αλυσίδα δικτύου και δεν θα μπορεί να αλλαχθεί.

Το απαραβίαστο σύστημα λογιστικών εγγράφων που ενισχύεται από το γεγονός ότι δεν υπάρχει ανάγκη για κουραστική γραφειοκρατία θα κάνει την όλη διαδικασία πιο βελτιωμένη. Όλα τα συναφή έξοδα που επιβαρύνθηκαν οι εταιρείες λόγω των προηγουμένως αναποτελεσματικών συστημάτων εφοδιαστικής αλυσίδας θα μειωθούν για να καταστήσουν το σύνολο των εργασιών πιο κερδοφόρο. [24]

1.2.3.10. Λιανικό εμπόριο

Με γνήσια προϊόντα να πωλούνται από το ένα σημείο του κόσμου στο άλλο, υπάρχει ένα μεγάλο πρόβλημα στην αποδείξει ότι τα προϊόντα είναι αυθεντικά. Σχεδόν 500 δισεκατομμύρια προϊόντα που δεν είναι γνήσια κυκλοφορούν παγκοσμίως κάθε χρόνο και οι καταναλωτές δεν ανέχονται πλέον αυτήν την παράλογη κατάσταση. Αυτό το πρόβλημα προκαλεί τεράστιες ζημιές στον χώρο του καταναλωτισμού αλλά μπορεί να λυθεί εύκολα με την τεχνολογία του Blockchain.

Το Blockchain περιλαμβάνει την αίσθηση της τήρησης των αρχείων από την αρχή της κατάστασης τους καθ΄ όλη την διάρκεια μέχρι την κατάληξή τους προσθέτοντας την προοπτική λογοκρισίας που δεν υπάρχει στον κλάδο του διαδικτυακού ηλεκτρονικού εμπορίου. Η τεχνολογία του Blockchain μπορεί να χρησιμοποιηθεί από χειριστές του λιανικού εμπορίου για να βεβαιωθούν πως τα προϊόντα που πουλάνε προέρχονται από τις αυθεντικές τους πηγές.

Τα εμπορεύματα λιανικής που λαμβάνονται από την πηγή τους με σκοπό να πωληθούν στους καταναλωτές, μπορούν να έχουν ετικέτες τις οποίες ο καταναλωτής θα σαρώνει για να δει την ιστορία του προϊόντος πριν την αγορά. Τα προϊόντα, όντας εγγεγραμμένα στο δίκτυο του Blockchain, θα βεβαιώνουν τον αγοραστή ότι το προϊόν δεν είναι κάποια απομίμηση ή παραποιημένο και ότι προήλθε όντως από την πηγή του. [24]

1.2.3.11. Βιομηχανία τυχερών παιχνιδιών

Με τις διαφορετικές δυνατότητες που προσφέρει το δίκτυο του Blockchain, δεν είναι δύσκολο να φανταστεί κάποιος να την εκμεταλλεύεται και η βιομηχανία τζόγου. Από τότε που ήρθε το διαδίκτυο στις ζωές των ανθρώπων, η σκέψη και μόνο του διαδικτυακού τζόγου είναι πολύ διάσημη. Ο διαδικτυακός τζόγος, προσφέροντας τις ευκαιρίες να απολαύσει κανείς τα αγαπημένα του παιχνίδια στο καζίνο ήταν αρχικά μια περίεργη ιδέα αλλά είναι πλέον μια κατηγορία από μόνη της στα καζίνο.

Με την ξαφνική εμφάνιση της τεχνολογίας του Blockchain, ο κόσμος του διαδικτυακού τζόγου έχει αλλάξει δραματικά. Τα κρυπτονομίσματα παρέχουν στις βιομηχανίες του τζόγου μια μέθοδος πληρωμής, που μπορεί να χρησιμοποιηθεί έναντι των κανονικών χρημάτων και τα πλεονεκτήματα αυτής της μεθόδου (δηλαδή να χρησιμοποιούνται εικονικά χρήματα αντί για κανονικά) είναι πολλά.

- Επιτρέπει στους παίχτες να παίξουν με τα λεφτά τους χωρίς να χρειάζεται να συμπληρώσουν προσωπικές φόρμες με τις πληροφορίες τους.
- Τα κρυπτονομίσματα κρατούν σημαντικά λιγότερες προμήθειες και παρέχουν γρήγορες καταθέσεις, έτσι γίνονται ιδανικά για τα μικρότερα κεφάλαια.
- Το γεγονός ότι τα κρυπτονομίσματα δεν ελέγχονται από νόμους σε συγκεκριμένες χώρες, έκανε τον τζόγο πιο προσιτό από ότι ήταν με το κανονικό χρήμα.

Τα κρυπτονομίσματα του Blockchain και η βιομηχανία του τζόγου, ταιριάζουν άψογα. Η Μάλτα σχεδιάζει να νομιμοποιήσει την χρήση του bitcoin στα διαδικτυακά καζίνο και αυτήν την στιγμή βλέπει τις καλύτερες επιλογές για να το κάνει πραγματικότητα.

Τέλος, με την εφαρμογή της τεχνολογίας του Blockchain στον τζόγο, ο τζόγος θα επωφεληθεί και από την διαφάνεια που δεν υπήρχε στο παρελθόν, πράγμα που κάνει τον τζόγο πιο δίκαιο. Χωρίς την πτυχή της λογοδοσίας, οι παίχτες δεν θα ήξεραν εάν το καζίνο παίζει σύμφωνα με τους κανόνες. [24]

1.2.3.12. Χιλιομετρική απάτη στα αυτοκίνητα

Η χιλιομετρική απάτη στα αυτοκίνητα είναι όταν κάποιος αλλάζει τον αριθμό των χιλιομέτρων που έχει ταξιδέψει ένα αυτοκίνητο. Με την παραβίαση αυτή, μπορεί κάποιος να κάνει ένα αυτοκίνητο να φαίνεται νεότερο και λιγότερο φθαρμένο, με αποτέλεσμα οι πελάτες να πληρώνουν περισσότερο από αυτό που πραγματικά αξίζει το αυτοκίνητο. Μάλιστα σε μερικές ευρωπαϊκές χώρες η πιθανότητα αγοράς ενός εισαγόμενου μεταχειρισμένου οχήματος

με “πειραγμένα” χιλιόμετρα αγγίζει το 80%, ενώ στην Ελλάδα το ποσοστό αγγίζει το 40% σύμφωνα με το lawspot.gr για το έτος 2018.

Οι κυβερνήσεις προσπαθούν να ανταπεξέλθουν σε αυτό, συλλέγοντας τα χιλιόμετρα των αυτοκινήτων κατά την διάρκεια της επιθεώρησης ασφαλείας, αλλά αυτό δεν αρκεί. Έτσι αντ’ αυτού θα μπορούσαν να αντικατασταθούν τα κανονικά χιλιομετρικά όργανα με έξυπνα, τα οποία θα συνδέονται με το διαδίκτυο και θα αναγράφουν τα χιλιόμετρα των αυτοκινήτων σε ένα blockchain. Αυτό θα δημιουργούσε ένα ασφαλές ψηφιακό πιστοποιητικό για κάθε αυτοκίνητο.

Και επειδή χρησιμοποιούν ένα Blockchain, κανείς δεν θα μπορεί να παραβιάσει τα δεδομένα αφού το Blockchain είναι αμετάβλητο και όλοι μπορούν να ψάξουν για το ιστορικό ενός οχήματος. Στην πραγματικότητα, αυτό αναπτύσσεται ήδη από την Bosch και το δοκιμάζουν αυτή τη στιγμή σε 100 αυτοκίνητα στη Γερμανία και την Ελβετία. Για αυτόν τον λόγο τα Blockchain είναι τέλεια για να παρακολουθούνται δεδομένα και να αποθηκεύουν τις αλλαγές τους με την πάροδο του χρόνου.

Αυτοί ήταν μόνο κάποιοι από τους τρόπους που μπορούμε να επωφεληθούμε από την τεχνολογία του Blockchain και επηρεάζει πολλές εταιρείες ανά τον κόσμο πέρα από την Fintech. Με ολοένα και περισσότερες εταιρείες και επιχειρηματίες να βοηθούν στην προώθηση του Blockchain, το μόνο που μένει είναι να δούμε μέχρι πόσο μπορούμε να το αξιοποιήσουμε και πόσο θα γίνει μέρος και θα επηρεάζει τις ζωές μας. [3]

2. ΟΙ ΔΥΟ ΓΙΓΑΝΤΕΣ ΚΑΙ ΤΑ ΣΤΑΘΕΡΑ ΝΟΜΙΣΜΑΤΑ

2.1. Bitcoin και Ethereum

Το Bitcoin είναι ένα αποκεντρωμένο ψηφιακό νόμισμα που δημιουργήθηκε τον Ιανουάριο του 2009. Ακολουθεί τις ιδέες που γράφτηκαν από τον μυστηριώδη με το ψευδώνυμο δημιουργό του Satoshi Nakamoto.

Η ταυτότητα του ατόμου ή των προσώπων που δημιούργησαν την τεχνολογία εξακολουθεί να είναι ένα μυστήριο. Το Bitcoin προσφέρει την υπόσχεση για χαμηλότερες χρεώσεις συναλλαγών από ό,τι οι παραδοσιακοί μηχανισμοί πληρωμών στο διαδίκτυο, και σε αντίθεση με τα νομίσματα που εκδίδονται από την κυβέρνηση, λειτουργεί από μια αποκεντρωμένη αρχή.

Το Bitcoin είναι γνωστό ως ένας τύπος κρυπτονομίσματος επειδή χρησιμοποιεί την κρυπτογραφία για να διατηρείται ασφαλές. Δεν υπάρχουν φυσικά bitcoin, μόνο συναλλαγές που τηρούνται σε ένα δημόσιο βιβλίο(public ledger) στο οποίο όλοι έχουν πρόσβαση (αν και κάθε εγγραφή είναι κρυπτογραφημένη). Όλες οι συναλλαγές Bitcoin επαληθεύονται από ένα τεράστιο ποσό υπολογιστικής ισχύος μέσω μιας διαδικασίας γνωστής ως «εξόρυξη»(mining). Το Bitcoin δεν εκδίδεται ούτε υποστηρίζεται από τράπεζες ή κυβερνήσεις, ούτε και ένα μεμονωμένο bitcoin είναι πολύτιμο ως εμπόρευμα. Παρά το γεγονός ότι δεν είναι νόμιμο

χρήμα στα περισσότερα μέρη του κόσμου, το Bitcoin είναι πολύ δημοφιλές και έχει προκαλέσει την κυκλοφορία εκατοντάδων άλλων κρυπτονομισμάτων, τα οποία συλλογικά αναφέρονται ως altcoins. Το Bitcoin συνήθως συντομεύεται ως BTC σε διαπραγματεύσεις.

Το σύστημα Bitcoin είναι μια συλλογή υπολογιστών (αναφέρονται επίσης ως "miners") που όλοι εκτελούν τον κώδικα του Bitcoin και αποθηκεύουν το blockchain του. Μεταφορικά μιλώντας, ένα blockchain μπορεί να θεωρηθεί ως μια συλλογή μπλοκ. Σε κάθε μπλοκ υπάρχει μια συλλογή από συναλλαγές. Επειδή όλοι οι υπολογιστές που εκτελούν το blockchain έχουν την ίδια λίστα μπλοκ και συναλλαγών, μπορούν να δουν αυτά τα νέα μπλοκ καθώς γεμίζουν με νέες συναλλαγές Bitcoin, έτσι κανείς δεν μπορεί να εξαπατήσει το σύστημα.

Οποιοσδήποτε—είτε εκτελεί έναν «κόμβο» Bitcoin είτε όχι— μπορεί να δει αυτές τις συναλλαγές να πραγματοποιούνται σε πραγματικό χρόνο. Για να επιτύχει μια εισβολή, ένας κακοποιός θα πρέπει να χειρίζεται το 51% της υπολογιστικής ισχύος που αποτελεί το Bitcoin. Το Bitcoin έχει περίπου 13.768 πλήρεις κόμβους, από τα μέσα Νοεμβρίου 2021, και αυτός ο αριθμός αυξάνεται, καθιστώντας μια τέτοια επίθεση αρκετά απίθανη.

Παρόλα αυτά, αν συνέβαινε μια επίθεση, οι εξορύκτες Bitcoin - οι άνθρωποι που συμμετέχουν στο δίκτυο Bitcoin με τους υπολογιστές τους - πιθανότατα θα χωρίζονταν σε ένα νέο blockchain, χρήζοντας την προσπάθεια που έκανε το κακοποιό στοιχείο για να πετύχει την επίθεση χαμένη.

Οι συναλλαγές που πραγματοποιούνται μέσω Bitcoin διατηρούνται χρησιμοποιώντας δημόσια και ιδιωτικά «κλειδιά», τα οποία είναι μεγάλες σειρές αριθμών και γραμμάτων που συνδέονται μέσω του μαθηματικού αλγόριθμου κρυπτογράφησης που τα δημιουργεί. Το δημόσιο κλειδί (συγκρίσιμο με αριθμό τραπεζικού λογαριασμού) χρησιμεύει ως η διεύθυνση που δημοσιεύεται στον κόσμο και στην οποία άλλοι μπορούν να στείλουν Bitcoin.

Το ιδιωτικό κλειδί (συγκρίσιμο με ένα PIN ATM) θα πρέπει να φυλάσσεται και χρησιμοποιείται μόνο για την εξουσιοδότηση μεταδόσεων Bitcoin. Τα κλειδιά Bitcoin δεν πρέπει να συγχέονται με ένα πορτοφόλι Bitcoin, το οποίο είναι μια φυσική ή ψηφιακή συσκευή που διευκολύνει τις συναλλαγές του bitcoin και επιτρέπει στους χρήστες να παρακολουθούν την ιδιοκτησία των νομισμάτων. Ο όρος "πορτοφόλι" είναι λίγο παραπλανητικός επειδή η αποκεντρωμένη φύση του Bitcoin σημαίνει ότι δεν αποθηκεύεται ποτέ «μέσα» σε ένα πορτοφόλι, αλλά καλύτερα διανέμεται σε μια αλυσίδα μπλοκ.

Το Ethereum είναι μια πλατφόρμα blockchain με το δικό της κρυπτονόμισμα, που ονομάζεται ether (ETH) ή ethereum, και έχει τη δική του γλώσσα προγραμματισμού, που ονομάζεται Solidity.

Ως δίκτυο Blockchain, το Ethereum έχει το δικό του αποκεντρωμένο δημόσιο βιβλίο για την επαλήθευση και την καταγραφή συναλλαγών. Οι χρήστες του δικτύου μπορούν να δημιουργούν, να δημοσιεύουν, να χρησιμοποιούν εφαρμογές στην πλατφόρμα και να

χρησιμοποιούν το κρυπτονόμισμα ether ως πληρωμή. Οι αποκεντρωμένες εφαρμογές του διαδικτύου αποκαλούνται "dApps".

Το Ethereum δημιουργήθηκε για να δώσει τη δυνατότητα στους προγραμματιστές να δημιουργούν και να δημοσιεύουν έξυπνες συμβάσεις(smart contracts) και κατανεμημένες εφαρμογές (dApps) που μπορούν να χρησιμοποιηθούν χωρίς τον κίνδυνο να διακοπεί η λειτουργίας τους, απάτης ή παρέμβασης από τρίτους.

Το Ethereum κυκλοφόρησε δημόσια τον Ιούλιο του 2015 από μια μικρή ομάδα λατρών του blockchain. Περιλάμβαναν τον Joe Lubin, ιδρυτή της ConsenSys, ενός προγραμματιστή εφαρμογών Blockchain που χρησιμοποιεί το δίκτυο Ethereum. Ένας άλλος συνιδρυτής, ο Vitalik Buterin, πιστεύεται ότι δημιούργησε την ιδέα του Ethereum και τώρα λειτουργεί ως Διευθύνων Σύμβουλος και ως το δημόσιο πρόσωπο του Ethereum. Ο Buterin είναι ο νεότερος crypto δισεκατομμυριούχος στον κόσμο.

Το κρυπτονόμισμα Ether σχεδιάστηκε για χρήση εντός του δικτύου Ethereum. Ωστόσο, όπως και το Bitcoin, το Ether είναι πλέον ένας αποδεκτός τρόπος πληρωμής από ορισμένους εμπόρους και προμηθευτές υπηρεσιών. Το Overstock, το Shopify και το CheapAir είναι μεταξύ των διαδικτυακών τοποθεσιών που δέχονται Ether ως πληρωμή.

Το Ethereum ισχυρίζεται ότι η πλατφόρμα του μπορεί να χρησιμοποιηθεί για την κωδικοποίηση, αποκέντρωση, ασφάλεια και διαπραγμάτευση σχεδόν οπουδήποτε. Μια σειρά από έργα βρίσκονται σε εξέλιξη για να δοκιμαστεί η ιδέα.

Η Microsoft συνεργάζεται με την ConsenSys για να προσφέρει το Ethereum Blockchain ως υπηρεσία (EBaaS) στο Microsoft Azure cloud. Προορίζεται να προσφέρει σε πελάτες και προγραμματιστές ένα περιβάλλον προγραμματιστών blockchain που βασίζεται στο cloud με ένα κλικ.

Το 2020, η Advanced Micro Devices (AMD) και η ConsenSys ανακοίνωσαν μια κοινή επιχείρηση για τη δημιουργία ενός δικτύου κεντρικών δεδομένων που θα βασίζονται στην υποδομή του Ethereum. [9]

2.2. Ethereum

Το Ethereum δημιουργήθηκε το 2013 από τον προγραμματιστή Vitalik Buterin. Το 2014, ξεκίνησαν οι εργασίες ανάπτυξης και χρηματοδοτήθηκαν από κοινού και το δίκτυο κυκλοφόρησε στις 30 Ιουλίου 2015. Η πλατφόρμα επιτρέπει σε οποιονδήποτε να αναπτύξει μόνιμες και αμετάβλητες αποκεντρωμένες εφαρμογές σε αυτό, με τις οποίες οι χρήστες μπορούν να αλληλοεπιδράσουν.

Το Ethereum περιεγράφηκε αρχικά σε ένα white paper από τον Vitalik Buterin, έναν προγραμματιστή και συνιδρυτή του Bitcoin Magazine στα τέλη του 2013, με στόχο τη δημιουργία αποκεντρωμένων εφαρμογών.

Ο Buterin υποστήριξε στους προγραμματιστές του πυρήνα του bitcoin, ότι το Bitcoin και η τεχνολογία blockchain θα μπορούσαν να επωφεληθούν και από άλλες εφαρμογές, εκτός από τα χρήματα, και χρειαζόταν μια πιο ισχυρή γλώσσα για την ανάπτυξη εφαρμογών που θα μπορούσε να οδηγήσει στη σύνδεση περιουσιακών στοιχείων του πραγματικού κόσμου, όπως μετοχές και ακίνητα μέσα από το blockchain.

Το 2013, ο Buterin συνεργάστηκε για λίγο με τον Διευθύνοντα Σύμβουλο της eToro, Yoni Assia, στο έργο Colored Coins και συνέταξε τη λευκή του βίβλο που περιγράφει πρόσθετες περιπτώσεις χρήσης για την τεχνολογία blockchain.

Ο Vitalik ωστόσο, αφού δεν κατάφερε να πετύχει μια συμφωνία σχετικά με τον τρόπο με τον οποίο θα προχωρήσει το έργο, πρότεινε την ανάπτυξη μιας νέας πλατφόρμας με μια πιο ισχυρή γλώσσα δέσμης ενεργειών—μια πλήρη γλώσσα προγραμματισμού Turing - η οποία τελικά θα γινόταν το Ethereum.

Οι εφαρμογές αποκεντρωμένων οικονομικών(DeFi) παρέχουν μια ευρεία γκάμα χρηματοοικονομικών υπηρεσιών, που να επιτρέπουν στους χρήστες κρυπτονομισμάτων να δανείζονται έναντι του λογαριασμού τους ή να τα δανείζουν για τόκους, χωρίς την ανάγκη από τρίτες υπηρεσίες, όπως χρηματιστηριακές εταιρείες, ανταλλακτήρια ή τράπεζες.

Το Ethereum επιτρέπει επίσης τη δημιουργία και την ανταλλαγή NFTs(Non Fungible Tokens), τα οποία είναι μη εναλλάξιμα tokens που συνδέονται με ψηφιακά έργα τέχνης ή άλλα αντικείμενα του πραγματικού κόσμου και πωλούνται ως μοναδική ψηφιακή ιδιοκτησία. Επιπλέον, πολλά άλλα κρυπτονομίσματα λειτουργούν ως tokens ERC-20 πάνω από το blockchain Ethereum και έχουν χρησιμοποιήσει την πλατφόρμα για ICOs(Initial Coin Offering).

Το Ethereum έχει αρχίσει να εφαρμόζει μια σειρά αναβαθμίσεων που ονομάζονται Ethereum 2.0, η οποία περιλαμβάνει μια μετάβαση στο proof of stake έναντι του proof of work και στοχεύει στην αύξηση της απόδοσης των συναλλαγών με την χρήση διαμοιρασμού.

Τον Ιανουάριο του 2018, το Ethereum είχε το δεύτερο μεγαλύτερο market capitalization, πίσω από το Bitcoin και το 2021, διατήρησε αυτή τη θέση. Το 2019, ο υπάλληλος του Ιδρύματος Ethereum Virgil Griffith συνελήφθη από την κυβέρνηση των ΗΠΑ για παρουσίαση σε συνέδριο blockchain στη Βόρεια Κορέα. Στις 27 Αυγούστου 2021, το blockchain παρουσίασε ένα hard fork που ήταν αποτέλεσμα των πελατών που εκτελούσαν διαφορετικές μη συμβατές εκδόσεις λογισμικού. [11]

Εικόνα 4: Ο δημιουργός του ethereum εξηγεί με δικά του λόγια το ethereum στο Disrupt SF[35]

2.2.1. NFT

Τα μη ανταλλάξιμα tokens ή NFTs είναι κρυπτογραφικά στοιχεία στο blockchain με μοναδικούς κωδικούς αναγνώρισης και μεταδεδομένα που τα διακρίνουν μεταξύ τους. Σε αντίθεση με τα κρυπτονομίσματα, τα NFTs δεν διαπραγματεύονται ούτε ανταλλάσσονται. Αυτό διαφέρει από tokens όπως τα κρυπτονομίσματα, τα οποία είναι πανομοιότυπα μεταξύ τους και επομένως μπορούν να χρησιμοποιηθούν ως μέσο για εμπορικές συναλλαγές.

Το κάθε ένα NFT είναι ξεχωριστό και μπορεί να χρησιμοποιηθεί για πολλούς διαφορετικούς σκοπούς. Για παράδειγμα, είναι ένα ιδανικό όχημα για την ψηφιακή αναπαράσταση φυσικών περιουσιακών στοιχείων όπως ακίνητα και έργα τέχνης. Επειδή βασίζονται σε blockchains, τα NFT μπορούν επίσης να χρησιμοποιηθούν για την αφαίρεση του μεσάζοντα(π.χ. μεσίτες) και τη σύνδεση καλλιτεχνών με το κοινό τους(π.χ. τραγουδιστές) ή για τη διαχείριση ταυτότητας του προϊόντος. Τα NFT μπορούν να αφαιρέσουν μεσάζοντες, να απλοποιήσουν τις συναλλαγές και να δημιουργήσουν νέες αγορές.

Μεγάλο μέρος της τρέχουσας αγοράς των NFT επικεντρώνεται σε συλλεκτικά αντικείμενα, όπως ψηφιακά έργα τέχνης, αθλητικές κάρτες και σπάνια αντικείμενα. Το NBA Top Shot είναι ένα μέρος όπου συλλέκτες κατέχουν NFT κάρτες του NBA με την μορφή ψηφιακών καρτών. Μερικές από αυτές τις κάρτες έχουν πουληθεί για εκατομμύρια δολάρια. Πρόσφατα, ο Διευθύνων Σύμβουλος του Twitter, Τζακ Ντόρσεϊ, δημοσίευσε στο Twitter έναν σύνδεσμο σε μορφή ενός token του πρώτου tweet που γράφτηκε ποτέ, όπου έγραψε " just setting up my twttr ". Η έκδοση NFT του πρώτου tweet έχει ήδη πωληθεί για 2.9 εκατομμύρια δολάρια.

Όπως το φυσικό χρήμα, τα κρυπτονομίσματα μπορούν να ανταλλαχθούν το ένα με το άλλο. Για παράδειγμα, ένα Bitcoin είναι πάντα ίσο σε αξία με ένα άλλο Bitcoin. Ομοίως, μια μεμονωμένη μονάδα Ether είναι πάντα ίση με μια άλλη μονάδα Ether. Αυτό το χαρακτηριστικό

ανταλλάξιμου καθιστά τα κρυπτονομίσματα κατάλληλα για χρήση ως ασφαλές μέσο συναλλαγών στην ψηφιακή οικονομία.

Τα NFT αλλάζουν το παραπάνω παράδειγμα κρυπτονομισμάτων, κάνοντας το κάθε ένα NFT μοναδικό και αναντικατάστατο, έτσι το κάθε ένα NFT δεν μπορεί να ισοδυναμεί με οποιοδήποτε άλλο NFT. Τα NFTs είναι ψηφιακές αναπαραστάσεις ψηφιακών στοιχείων και παρομοιάζονται με ψηφιακά διαβατήρια, επειδή το κάθε ένα NFT περιέχει και έναν μοναδικό κωδικό που το κάνει να ξεχωρίζει από τα υπόλοιπα. Είναι επίσης επεκτάσιμα που σημαίνει ότι με δύο διαφορετικά NFT μπορεί να δημιουργηθεί ένα τρίτο που θα είναι ο συνδυασμός των δύο.

Τα NFT όπως και το Bitcoin, περιέχουν πληροφορίες ιδιοκτησίας για να αναγνωρίζονται και να μεταφέρονται εύκολα. Οι ιδιοκτήτες μπορούν να προσθέσουν μεταδεδομένα ή χαρακτηριστικά που σχετίζονται με το συγκεκριμένο στοιχείο του NFT. Για παράδειγμα, τα tokens αντιπροσωπεύουν τους κόκκους καφέ και μπορούν να θεωρηθούν ως fair trades ή ένας καλλιτέχνης μπορεί να υπογράψει το ψηφιακό του δίκτυο με την δική του υπογραφή σε ένα μεταδεδομένο.

Τα NFT εξελίχθηκαν από το πρότυπο ERC-721. Αναπτύχθηκε από τους ανθρώπους που ήταν υπεύθυνοι για το έξυπνο συμβόλαιο του ERC-20. Το ERC-721 ορίζει την ελάχιστη διεπαφή (λεπτομέρειες ιδιοκτησίας, ασφάλεια και μεταδεδομένα) που απαιτούνται για την ανταλλαγή και τη διανομή token παιχνιδιών. Το πρότυπο ERC-1155 προωθεί την ιδέα περαιτέρω μειώνοντας το κόστος συναλλαγής και αποθήκευσης που απαιτούνται για τα NFT και ομαδοποιεί πολλαπλούς τύπους NFT σε ένα ενιαίο συμβόλαιο.

Ίσως η πιο διάσημη περίπτωση χρήσης για τα NFT είναι αυτή των cryptokitties. Τα cryptokitties που κυκλοφόρησαν τον Νοέμβριο του 2017 είναι ψηφιακές αναπαραστάσεις γατών με μοναδικές ταυτότητες στο blockchain του Ethereum. Κάθε γατάκι είναι μοναδικό και έχει μια τιμή που αναπαρίσταται με Eth. Αναπαράγονται μεταξύ τους και παράγουν νέους απογόνους, οι οποίοι έχουν διαφορετικές ιδιότητες και αποτιμήσεις σε σύγκριση με τους γονείς τους. Μέσα σε λίγες εβδομάδες από την κυκλοφορία τους, τα cryptokitties συγκέντρωσαν θαυμαστές που ξόδεψαν 20 εκατομμύρια δολάρια σε Eth για την αγορά, τη διατροφή και την ανατροφή τους. Μερικοί λάτρεις ξόδεψαν ακόμη και πάνω από 100.000 $.

Ενώ η περίπτωση χρήσης cryptokitties μπορεί να ακούγεται ασήμαντη, στα επόμενα βλέπουμε πιο σοβαρές επιχειρηματικές περιπτώσεις. Για παράδειγμα, τα NFTs έχουν χρησιμοποιηθεί σε συναλλαγές ιδιωτικών μετοχών καθώς και σε συμφωνίες ακινήτων. Μία από τις συνέπειες της ενεργοποίησης πολλαπλών τύπων tokens σε ένα συμβόλαιο είναι η δυνατότητα παροχής μεσεγγύησης για διαφορετικούς τύπους NFT, από έργα τέχνης έως ακίνητα, σαν μια ενιαία οικονομική συναλλαγή.

Τα NFTs είναι μια εξέλιξη σχετικά με την απλή έννοια των κρυπτονομισμάτων. Τα σύγχρονα χρηματοοικονομικά συστήματα αποτελούνται από εξελιγμένα συστήματα συναλλαγών και δανείων για διαφορετικούς τύπους περιουσιακών στοιχείων, που

κυμαίνονται από ακίνητα έως δανειστικές συμβάσεις μέχρι και έργα τέχνης. Επιτρέποντας ψηφιακές αναπαραστάσεις φυσικών περιουσιακών στοιχείων, τα NFT αποτελούν ένα βήμα προς τα εμπρός στην επανεφεύρεση αυτής της υποδομής.

Σίγουρα, η ιδέα ψηφιακών αναπαραστάσεων των φυσικών περιουσιακών στοιχείων και η χρήση μοναδικής αναγνώρισης δεν είναι καινοφανής, αλλά αν αυτές οι έννοιες συνδυαστούν με τα πλεονεκτήματα ενός smart contract πάνω σε ένα blockchain, τότε μπορούν να γίνουν μια δύναμη που μπορεί να αλλάξει τον τρόπο που βλέπουμε τα πράγματα.

Μπορεί η πιο προφανές περίπτωση των NFT να είναι η αποτελεσματικότητα της αγοράς. Η μετατροπή ενός φυσικού περιουσιακού στοιχείου σε ψηφιακό εξορθολογίζει τις διαδικασίες και αφαιρεί το κομμάτι του μεσάζοντα. Τα NFT που αντιπροσωπεύουν ψηφιακά ή φυσικά έργα τέχνης σε ένα blockchain αφαιρούν την ανάγκη για μεσάζοντα και επιτρέπουν στους καλλιτέχνες να συνδέονται απευθείας με το κοινό τους καθώς μπορούν να βελτιώσουν τις όποιες επιχειρηματικές τους διαδικασίες. Για παράδειγμα, ένα NFT για ένα μπουκάλι κρασί θα διευκολύνει τον καταναλωτή να μάθει από που παράχθηκε, που ήταν πριν, πόσο στοίχιζε με την πάροδο του χρόνου, κ.α.. Υπάρχουν εταιρείες όπως η Ernst & Young η οποία έχει ήδη αναπτύξει μια τέτοια λύση για τους πελάτες της.

Η μοναδική ταυτότητα και η ιδιοκτησία ενός NFT είναι μπορεί να επαληθευτεί μέσα από το blockchain. Η ιδιοκτησία του NFT συνδέεται συχνά με άδεια χρήσης του υποκείμενου ψηφιακού στοιχείου, αλλά γενικά δεν εκχωρεί πνευματικά δικαιώματα στον αγοραστή. Ορισμένες συμφωνίες χορηγούν άδεια μόνο για προσωπική, μη εμπορική χρήση, ενώ άλλες άδειες επιτρέπουν επίσης την εμπορική χρήση του υποκειμενικού ψηφιακού περιουσιακού στοιχείου.

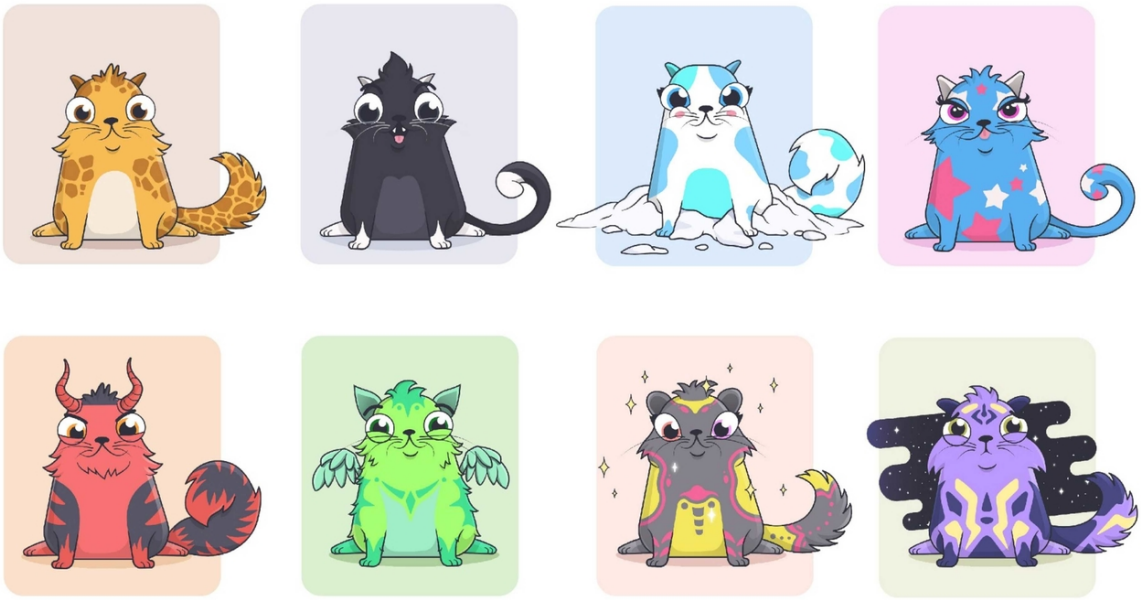
Τα NFT μπορούν επίσης να εκδημοκρατίσουν τις επενδύσεις κλασματοποιώντας φυσικά περιουσιακά στοιχεία όπως τα ακίνητα. Είναι πολύ πιο εύκολο να διαιρεθεί ένα ψηφιακό ακίνητο μεταξύ πολλών ιδιοκτητών. Ένας πίνακας δεν θα χρειάζεται να ανήκει σε ένα μόνο άτομο αλλά ο κάθε ένας θα μπορεί να αγοράσει ένα «κομμάτι» του πίνακα. Έτσι γίνεται και να αυξηθεί η αξία του πίνακα αλλά και τα έσοδα που προέρχονται από τα συγκεκριμένα ακίνητα.

Κάποιες ιδιωτικές διαδικτυακές κοινότητες έχουν δημιουργηθεί γύρω από την ιδιοκτησία ορισμένων εκδόσεων NFT. Οι εικονικοί κόσμοι όπως η Decentraland, το Sandbox, το Star Atlas, τα CryptoVoxels και το Somnium Space επιτρέπουν στους χρήστες να δημιουργούν γκαλερί για να επιδεικνύουν την τέχνη NFT και τα αντικείμενα του παιχνιδιού NFT. Τα NFT έχουν χρησιμοποιηθεί για τη δημοπρασία εικονικής γης εντός των παιχνιδιών. Τον Ιούνιο του 2021, ένα οικόπεδο εικονικής γης μεγέθους 16 στρεμμάτων στο Decentraland πωλήθηκε για 913.228,20 $.

Οι πιο συναρπαστικές δυνατότητες των NFT, είναι αυτές των νέων μορφών επενδύσεων αλλά και των νέων αγορών. Ένα κομμάτι ακίνητης περιουσίας χωρισμένο σε πολλαπλά τμήματα, που το καθένα από αυτά περιέχει διαφορετικά χαρακτηριστικά και

τύπους ιδιοκτησίας όπως για παράδειγμα μερικά τμήματα μπορεί να είναι δίπλα από μια παραλία ή άλλα να είναι μέρη ψυχαγωγίας θα μπορούν να έχουν διαφορετική χρέωση και πολλούς ιδιοκτήτες. Το εμπόριο ακινήτων, μια περίπλοκη και γραφειοκρατική υπόθεση, μπορεί να απλοποιηθεί με την ενσωμάτωση σχετικών μεταδεδομένων σε κάθε μοναδικό NFT.

Η Decentraland, μια πλατφόρμα εικονικής πραγματικότητας στο blockchain του Ethereum, έχει ήδη εφαρμόσει μια τέτοια ιδέα. Καθώς τα NFT γίνονται πιο εξελιγμένα και ενσωματώνονται στην χρηματοοικονομική υποδομή, μπορεί να καταστεί δυνατή η εφαρμογή της ίδιας ιδέας κάποιων τεμαχίων που διαφέρουν σε αξία και τοποθεσία, στον φυσικό κόσμο. [13, 14, 36]



Εικόνα 5: Τα διάσημα Cryptokitties NFT[36]

2.3. Stablecoins

Ένα stablecoin είναι μια κατηγορία κρυπτονομισμάτων η οποία προσπαθεί να φέρει σταθερότητα στις τιμές τους και υποστηρίζονται από ένα τεράστιο αποθεματικό περιουσιακό στοιχείο. Τα stablecoins έχουν κερδίσει την έλξη πολλών επενδυτών καθώς προσφέρουν το καλύτερο για την οικονομία, δηλαδή την άμεση εξυπηρέτηση, την ασφάλεια και την ανωνυμία των πληρωμών των κρυπτονομισμάτων με σταθερές αποτιμήσεις νομισμάτων fiat(γενικά, με τον όρο fiat εννοείται το “ρευστό” το χρήμα) χωρίς μεταβλητότητα.

Τα stablecoins είναι κρυπτονομίσματα που προσπαθούν να συνδέσουν την αξία τους στην αγορά με κάποια εξωτερική αναφορά. Συνδέονται με νομίσματα fiat(δολάριο, ευρώ, γεν) ή με τιμές εμπορευμάτων, όπως ο χρυσός και το ασήμι ή το λάδι. Τα stablecoins επιτυγχάνουν τη σταθερότητα των τιμών τους μέσω εξασφάλισης (backing) ή μέσω αλγοριθμικών

μηχανισμών αγοράς και πώλησης του περιουσιακού στοιχείου αναφοράς ή των παραγώγων του.

Παρότι το Bitcoin είναι το πιο δημοφιλές νόμισμα, τείνει να υποφέρει από την υψηλή αστάθεια στις αποτιμήσεις του. Για παράδειγμα, η αξία του ανέβηκε από τα 5 χιλιάδες δολάρια στην περίοδο της πανδημίας του Μαρτίου του 2020 σε περίπου 65 χιλιάδες τον Απρίλιο του 2021 και μειώθηκε 50 τις εκατό κοντά στις 30 χιλιάδες ενώ η τιμή του πέρασε τις 65 χιλιάδες τον Νοέμβρη του 2021. Μέχρι και οι ημερήσιες διακυμάνσεις της τιμής του μπορεί να είναι ασταθείς. Είναι σύνηθες κάποιο κρυπτονόμισμα να κυμαίνεται 10% προς οποιαδήποτε κατεύθυνση μέσα σε λίγες μόλις ώρες.

Αυτή η βραχυπρόθεσμη αστάθεια καθιστά τα κρυπτονομίσματα ακατάλληλα για καθημερινή χρήση. Ουσιαστικά, ένα νόμισμα θα πρέπει να λειτουργεί ως ένα μέσο νομισματικής ανταλλαγής και ως μέσο αποθήκευσης της νομισματικής αξίας καθώς η αξία του θα πρέπει να παραμένει σχετικά σταθερή κατά μεγάλα χρονικά διαστήματα. Οι επενδυτές θα αποφεύγουν να το αγοράσουν αν δεν είναι σίγουροι για την μελλοντική του αξία.

Ιδανικά, ένα κρυπτονόμισμα θα πρέπει να διατηρεί την αγοραστική του αξία και να έχει την μικρότερο δυνατό πληθωρισμό αρκετό για να ενθαρρύνει να δαπανούν οι χρήστες τα κρυπτονομίσματά τους αντί να τα αποθηκεύουν. Τα stablecoins παρέχουν μια λύση για την επίτευξη αυτού.

Υπάρχει μια απήχηση μεταξύ των νομισμάτων fiat, όπως είναι το αμερικανικό δολάριο, όπου το νόμισμα υποστηρίζεται από την πλήρη πίστη των καταναλωτών και την υποστήριξη της κυβέρνησης πίσω από αυτό. Αυτό προφέρει στο νόμισμα κάποια σταθερότητα στις τιμές του. Ωστόσο, αυτό σημαίνει πως πολλά νομίσματα fiat ελέγχονται φυσικά από τις κεντρικές τους τράπεζες. Τα stablecoins προσπαθούν να γεφυρώσουν αυτό το χάσμα μεταξύ των fiat νομισμάτων και των κρυπτονομισμάτων.

Τα αποθέματα που συλλέγονται, κρατούνται από ανεξάρτητους θεματοφύλακες και ελέγχονται τακτικά. Το Tether (USDTUSD) και το TrueUSD (TUSDUSD) είναι δημοφιλή κρυπτονομίσματα που έχουν αξία περίπου ισοδύναμη με αυτή ενός δολαρίου ΗΠΑ και υποστηρίζονται από καταθέσεις σε δολάρια. Τον Ιανουάριο του 2021, το stablecoin Tether είχε το τέταρτο μεγαλύτερο σε market capital(αριθμό συνολικών χρημάτων) όλων των κρυπτονομισμάτων. Τα stablecoins χωρίζονται σε τρεις κατηγορίες, όλες με βάση τους μηχανισμούς λειτουργείας τους: [30]

2.3.1. Ασφαλισμένα stablecoins

Τα stablecoins που έχουν εξασφαλισμένη κρυπτογράφηση υποστηρίζονται από άλλα κρυπτονομίσματα. Επειδή το αποθεματικό κρυπτονομίσματος μπορεί επίσης να είναι επιρρεπές σε υψηλή μεταβλητότητα, αυτού του είδους τα stablecoins έχουν πολύ μεγάλη

ασφάλεια, δηλαδή, διατηρείται μεγαλύτερος αριθμός των tokens τους ως αποθεματικό για την έκδοση μικρότερου αριθμού stablecoin.

Για παράδειγμα τέτοια τα stablecoins, μπορούν να εξασφαλίσουν δύο χιλιάδες δολάρια σε μορφή ether για να εκδοθούν χίλια δολάρια με την βοήθεια της κρυπτογράφησης τα οποία θα φιλοξενούν το 50% του αποθεματικού του ether. Όσο περισσότεροι και συχνότεροι έλεγχοι γίνονται και όσο ποιο συχνά παρακολουθούνται, τόσο πιο σταθερό είναι το κρυπτονόμισμα. Υποστηριζόμενο από το δίκτυο του Ethereum(ETHUSD), το DAI(DAIUSD) της MakerDAO είναι συνδεδεμένο με το δολάριο των ΗΠΑ και επιτρέπει την χρήση κρυπτογραφημένων περιουσιακών στοιχείων ως αποθεματικά. [30]

2.3.2. Μη ασφαλισμένα stablecoins

Τα μη ασφαλισμένα stablecoin δεν χρησιμοποιούν κανένα αποθεματικό, αλλά περιλαμβάνουν έναν λειτουργικό μηχανισμό, όπως αυτός μιας τράπεζας, για τη διατήρηση της σταθερής τιμής. Για παράδειγμα, το βασικό νόμισμα συνδεδεμένο με το δολάριο χρησιμοποιεί έναν μηχανισμό συναίνεσης για να αυξήσει ή να μειώσει την προσφορά κουπονιών ανάλογα με τις ανάγκες.

Αυτές οι ενέργειες είναι παρόμοιες με την εκτύπωση των τραπεζογραμματίων από μια κεντρική τράπεζα για τη διατήρηση των αποτιμήσεων του νομίσματος fiat. Μπορεί να επιτευχθεί με την εφαρμογή ενός έξυπνου συμβολαίου σε μια αποκεντρωμένη πλατφόρμα που μπορεί να λειτουργεί με κάποιον αυτόνομο τρόπο. [30]

2.3.3. Ρυθμισμένα stablecoins

Τα stablecoin ελέγχονται από τις ρυθμιστικές αρχές, δεδομένου του μεγέθους της αγοράς τους να αγγίζει τα 130 δισεκατομμύρια δολάρια και του πιθανού αντίκτυπου στο ευρύτερο χρηματοπιστωτικό σύστημα. Τον Οκτώβριο του 2021, ο Διεθνής Οργανισμός Επιτροπών Κινητών Αξιών είπε ότι τα stablecoins θα πρέπει να ρυθμίζονται ως υποδομή χρηματοπιστωτικής αγοράς παράλληλα με τα συστήματα πληρωμών και τα κέντρα εκκαθάρισης. Οι προτεινόμενοι κανόνες θα στοχεύουν συγκεκριμένα τα stablecoins που οι ρυθμιστικές αρχές θεωρούν σημαντικά και που έχουν τη δυνατότητα να διακόπτουν τις συναλλαγές πληρωμών και διακανονισμού.

Επιπλέον, ορισμένοι πολιτικοί έχουν αυξήσει τις εκκλήσεις τους για να υπάρξει μεγαλύτερη εποπτεία των stablecoin. Για παράδειγμα, τον Σεπτέμβριο του 2021, η γερουσιαστής Cynthia Lummis (R-Wyoming) ζήτησε τακτικούς ελέγχους από τους εκδότες ορισμένων stablecoin, ενώ άλλοι επιθυμούν να υπάρξουν τραπεζικοί κανονισμοί για αυτά. [30]

Εικόνα 6: Τα 3 πιο δημοφιλή stablecoins (από πάνω): DAI, USD Coin, Tether[37]

2.4. Decentralized Autonomous Organization (DAO)

Ένα από τα κύρια χαρακτηριστικά των κρυπτονομισμάτων είναι ότι είναι αποκεντρωμένα. Αυτό σημαίνει ότι δεν ελέγχονται από κάποιο μεμονωμένο ίδρυμα, όπως μια κυβέρνηση ή μια κεντρική τράπεζα, αλλά αντιθέτως χωρίζονται σε μια ποικιλία υπολογιστών, δικτύων και κόμβων. Σε πολλές περιπτώσεις, τα εικονικά νομίσματα κάνουν χρήση αυτής της αποκέντρωσης για να επιτύχουν επίπεδα απορρήτου και ασφάλειας που συνήθως δεν είναι διαθέσιμα στα τυπικά νομίσματα και στις συναλλαγές τους.

Εμπνευσμένοι από την αποκέντρωση των κρυπτονομισμάτων, μια ομάδα προγραμματιστών σκέφτηκε την ιδέα για έναν αποκεντρωμένο αυτόνομο οργανισμό(DAO), το 2016. Το DAO ήταν ένας οργανισμός που δημιουργήθηκε από προγραμματιστές για να αυτοματοποιήσει τις αποφάσεις και να διευκολύνει τις συναλλαγές κρυπτονομισμάτων. Τον Ιούνιο του 2016, λόγω σφαλμάτων προγραμματισμού και φορέων επίθεσης, χάκερ επιτέθηκαν στο DAO, αποκτώντας πρόσβαση σε 3,6 εκατομμύρια ethereum. Τα νομίσματα ψηφιακών συναλλαγών διέγραψαν το διακριτικό του DAO τον Σεπτέμβριο του 2016.

Το DAO ήταν ένας οργανισμός που σχεδιάστηκε για να είναι αυτοματοποιημένος και αποκεντρωμένος. Λειτουργούσε ως μια μορφή ταμείου επιχειρηματικού κεφαλαίου, ανοιχτού κώδικα και χωρίς τυπική δομή διαχείρισης ή διοικητικό συμβούλιο. Για να είναι πλήρως αποκεντρωμένο, το DAO δεν ήταν συνδεδεμένο με κάποιο συγκεκριμένο έθνος-κράτος και έκανε χρήση του δικτύου Ethereum.

Οι δημιουργοί του DAO πιστεύουν ότι μπορούν να εξαλείψουν τον παράγοντα του ανθρώπινου λάθους και την χειραγώγηση των κεφαλαίων των επενδυτών θέτοντας την

εξουσία των λήψεων των αποφάσεων στα χέρια ενός αυτοματοποιημένου συστήματος και μιας διαδικασίας crowdsource. Τροφοδοτούμενο με το token του Ethereum, το DAO σχεδιάστηκε για να επιτρέπει στους επενδυτές την αποστολή χρημάτων από οπουδήποτε στον κόσμο σε οποιονδήποτε ανώνυμα. Στη συνέχεια, το DAO θα παρείχε σε αυτούς τους ιδιοκτήτες, tokens, επιτρέποντάς τους τα δικαιώματα της ψήφου σε μελλοντικά έργα.

Το DAO κυκλοφόρησε στα τέλη του Απριλίου το 2016 χάρη στο μεγάλο πλήθος των token που συγκεντρώθηκε σε ένα μήνα, με περισσότερα από 150 εκατομμύρια δολάρια με την μορφή κεφαλαίων. Εκείνη την εποχή αυτό το λανσάρισμα είχε την μεγαλύτερη εκστρατεία συγκέντρωσης χρημάτων.

Μέχρι τον Μάιο του 2016, το DAO κατείχε ένα τεράστιο ποσοστό όλων των ether token που είχαν εκδοθεί μέχρι εκείνο το σημείο, έως και 14% όπως αναφέρει το περιοδικό The Economist. Την ίδια στιγμή ωστόσο, δημοσιεύτηκε ένα έγγραφο που περιείχε πολλά πιθανά τρωτά σημεία, προειδοποιώντας τους επενδυτές σε μελλοντικά επενδυτικά σχέδια μέχρις ότου τα τρωτά αυτά σημεία να επιλυθούν.

Αργότερα, τον Ιούνιο του 2016, μερικοί χάκερ επιτέθηκαν στο DAO με βάση αυτά τα τρωτά σημεία. Οι χάκερ απέκτησαν πρόσβαση σε 3.6 εκατομμύρια ethereum με συνολική αξία περίπου 50 εκατομμυρίων δολαρίων εκείνης της εποχής. Αυτό προκάλεσε μια τεράστια και αμφιλεγόμενη διαφωνία μεταξύ των επενδυτών του DAO, με μερικά άτομα να προτείνουν διάφορους τρόπους αντιμετώπισης του χακαρίσματος και άλλους να ζητούν την διάλυσή του. Το συγκεκριμένο περιστατικό έπαιξε μεγάλο ρόλο στο hard forking του δικτύου του Ethereum το οποίο έλαβε χώρα σύντομα.

Σύμφωνα με το IEEE Spectrum, το DAO είχε προγραμματιστικά λάθη και ήταν ευάλοτο σε vector επιθέσεις. Το γεγονός ότι ο οργανισμός σχεδίαζε όσον αφορά τους κανονισμούς, νέα εδάφη και το εταιρικό δίκαιο δεν έκανε την διαδικασία πιο εύκολη.

Οι συνέπειες της δομής του οργανισμού ήταν πολυάριθμες: οι επενδυτές ανησυχούσαν ότι θα θεωρούνταν υπεύθυνοι για τις ενέργειες που έπραξε το DAO ως ευρύτερος οργανισμός.

Το DAO επίσης δρούσε ύπουλα σχετικά με το αν πουλούσε τίτλους. Επιπλέον, υπήρχαν μακροχρόνια ζητήματα σχετικά με τον τρόπο λειτουργίας του DAO στον πραγματικό κόσμο. Οι επενδυτές και οι δημιουργοί χρειάζονταν να μετατρέψουν το ETH σε νομίσματα fiat, και αυτό θα μπορούσε να επηρεάσει αρνητικά την αξία του νομίσματος ethereum.

Μετά την διαμάχη για το μέλλον του DAO και το περιστατικό του hacking πριν από λίγους μήνες, πολλά διάσημα ανταλλακτήρια διέγραψαν το token του DAO, σηματοδοτώντας το τέλος του όπως είχε αρχικά οραματιστεί. Τον Ιούλιο του 2017, η Επιτροπή Κεφαλαιαγοράς (SEC) εξέδωσε μια έκθεση, στην οποία διαπιστώθηκε ότι το DAO πούλησε τίτλους με τη μορφή token στο blockchain του Ethereum, παραβιάζοντας τμήματα της νομοθεσίας περί τίτλων των ΗΠΑ.

Το DAO όπως είχε αρχικά οραματιστεί, δεν είχε επιστρέψει μέχρι τα μέσα του 2020, ωστόσο το ενδιαφέρων για τους αποκεντρωμένους αυτόνομους οργανισμούς αυξανόταν. Το 2021, το The Maker Foundation, ένα σύμβολο της βιομηχανίας των κρυπτονομισμάτων, ανακοίνωσε επίσημα ότι παρέδιδε τις λειτουργίες του στο MakerDAO, δημιουργό του σταθερού κρυπτονομίσματος DAI και ότι θα διαλύονταν μέχρι το τέλος του έτους.

Ενώ υπάρχουν πολλές ανησυχίες και πιθανά ζητήματα σχετικά με την νομιμότητα, την ασφάλεια και την δομή, κάποιοι αναλυτές και επενδυτές πιστεύουν ότι αυτού του είδους οργάνωσης θα αναδειχθεί τελικά και μπορεί ακόμα και να αντικαταστήσει τις παραδοσιακές επιχειρήσεις. Το δημοφιλές ψηφιακό νόμισμα Dash είναι ένα παράδειγμα ενός αποκεντρωμένου αυτόνομου οργανισμού, λόγω του τρόπου της διακυβέρνησής του, του τρόπου με τον οποίο είναι δομημένο το σύστημα προϋπολογισμού του και ίσως είναι μόνο θέμα χρόνου μέχρι να εισέλθουν επιπλέον DAOs στο πεδίο των κρυπτονομισμάτων. [29, 30]

3. ΧΡΗΣΙΜΟΤΗΤΑ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

3.1. Εξόρυξη

Η εξόρυξη bitcoin είναι η διαδικασία με την οποία νέα bitcoin τίθενται σε κυκλοφορία. Είναι επίσης ο τρόπος με τον οποίο επιβεβαιώνονται οι νέες συναλλαγές από το δίκτυο και αποτελεί κρίσιμο στοιχείο της συντήρησης και ανάπτυξης του blockchain. Η “εξόρυξη” εκτελείται με χρήση εξελιγμένου υλικού που λύνει ένα εξαιρετικά πολύπλοκο υπολογιστικό μαθηματικό πρόβλημα. Στον πρώτο υπολογιστή που θα βρει τη λύση στο πρόβλημα απονέμεται το επόμενο μπλοκ bitcoin καθώς και μια αμοιβή σε μορφή bitcoin.

Η εξόρυξη κρυπτονομισμάτων γίνεται προσεκτικά, είναι επίπονη, δαπανηρή και μόνο σποραδικά ανταποδοτική. Ωστόσο, η εξόρυξη έχει έλξει πολλούς επενδυτές που ενδιαφέρονται για κρυπτονομίσματα, λόγω του γεγονότος ότι οι εξορύκτες ανταμείβονται για τη δουλειά τους με κρυπτονομίσματα. Αυτό μπορεί να οφείλεται στο ότι οι επιχειρηματίες βλέπουν την εξόρυξη σαν φλουριά, όπως οι ανιχνευτές χρυσού στην Καλιφόρνια το 1849.

Οι περισσότεροι λόγοι για να γίνει το mining είναι η προοπτική ότι υπάρχει η ανταμοιβή με Bitcoin. Σίγουρα δεν χρειάζεται να είναι κάποιος εξορύκτης για να έχει τα tokens των κρυπτονομισμάτων. Τα κρυπτονομίσματα πωλούνται επίσης και ανταλλάσσονται εύκολα με την χρήση κανονικού χρήματος. Μπορούν να ανταλλαχθούν σε ένα ανταλλακτήριο όπως το Bitstamp χρησιμοποιώντας άλλη κρυπτογράφηση (για παράδειγμα, χρησιμοποιώντας Ethereum ή NEO και να ανταλλαχθεί με Bitcoin) ή το Binance. Μπορεί ακόμη να κερδηθεί κάνοντας αγορές, δημοσιεύοντας αναρτήσεις ιστολογίου σε πλατφόρμες που πληρώνουν τους χρήστες σε κρυπτονομίσματα ή ακόμη και δημιουργώντας λογαριασμούς κρυπτονομισμάτων που κερδίζουν κάποιους τόκους κάνοντας staking.

Ένα παράδειγμα πλατφόρμας ιστολογίου κρυπτογράφησης είναι το Steemit, το οποίο μοιάζει με το Medium, με τη διαφορά ότι οι χρήστες μπορούν να ανταμείψουν τους blogger

πληρώνοντάς τους σε ένα αποκλειστικό κρυπτονόμισμα που ονομάζεται STEEM. Στη συνέχεια, το STEEM μπορεί να διαπραγματευτεί αλλού για Bitcoin.

Η ανταμοιβή Bitcoin που λαμβάνουν οι εξορύκτες είναι το κίνητρο που παρακινεί τους ανθρώπους να βοηθούν στον πρωταρχικό σκοπό της εξόρυξης δηλαδή, να νομιμοποιήσουν και να παρακολουθούν τις συναλλαγές Bitcoin, διασφαλίζοντας την εγκυρότητά τους. Επειδή αυτές οι ευθύνες κατανέμονται μεταξύ πολλών χρηστών σε όλο τον κόσμο, το Bitcoin είναι ένα «αποκεντρωμένο» κρυπτονόμισμα ή ένα κρυπτονόμισμα που δεν βασίζεται σε καμία κεντρική αρχή όπως μια κεντρική τράπεζα ή μια κυβέρνηση για την επίβλεψη και την ρύθμισή του.

Οι miners πληρώνονται για τη δουλειά τους ως ελεγκτές. Επαληθεύουν την εγκυρότητα των συναλλαγών Bitcoin. Αυτό έχει σκοπό να κρατά τους χρήστες του Bitcoin ειλικρινείς μεταξύ τους και σχεδιάστηκε από τον/τους ιδρυτή/ες του Bitcoin, Satoshi Nakamoto. Με την επαλήθευση των συναλλαγών, οι εξορύκτες βοηθούν στην αποφυγή του "προβλήματος της διπλής δαπάνης".

Η διπλή δαπάνη είναι ένα σενάριο στο οποίο ένας ιδιοκτήτης Bitcoin ξοδεύει παράνομα το ίδιο bitcoin δύο φορές. Με το φυσικό νόμισμα, αυτό δεν είναι πρόβλημα. Για παράδειγμα, μόλις δοθεί ένα χαρτονόμισμα των 20 ευρώ σε έναν λογαριασμό για μία συναλλαγή, δεν γίνεται να ξαναχρησιμοποιηθεί για μια άλλη συναλλαγή, και επομένως δεν υπάρχει κίνδυνος να χρησιμοποιηθεί το ίδιο χαρτονόμισμα για την αγορά κάποιου άλλου αγαθού. Ενώ υπάρχει η πιθανότητα δημιουργίας πλαστών μετρητών, δεν είναι ακριβώς το ίδιο με το να ξοδευτεί κυριολεκτικά το ίδιο δολάριο δύο φορές.

Με το ψηφιακό νόμισμα, ωστόσο, όπως εξηγεί το λεξικό της Investopedia, “υπάρχει κίνδυνος ο κάτοχος να δημιουργήσει ένα αντίγραφο του ψηφιακού διακριτικού και να το στείλει σε έναν έμπορο ή κάπου αλλού διατηρώντας το πρωτότυπο”.

Αν για παράδειγμα υπήρχε ένα νόμιμο χαρτονόμισμα των 20 ευρώ και ένα πλαστό των ίδιων 20 ευρώ και προσπαθούσε να ξοδευτεί τόσο τον πραγματικό όσο και τον πλαστό, κάποιος που μπήκε στον κόπο να κοιτάξει και τους δύο σειριακούς αριθμούς λογαριασμών θα έβλεπε ότι ήταν ο ίδιος αριθμός, και επομένως ένας από αυτούς πρέπει να είναι ψεύτικος. Αυτό που κάνει ένας εξορύκτης Bitcoin είναι ανάλογο με αυτό—ελέγχει τις συναλλαγές για να βεβαιωθεί ότι οι χρήστες δεν προσπάθησαν παράνομα να ξοδέψουν το ίδιο bitcoin δύο φορές.

Παρότι μπορεί κανείς να είναι miner και να κάνει mining στο δίκτυο Bitcoin, δεν εγγυάται ότι θα αποκτήσει και tokens(BTC). Μόνο αυτός που θα τελειώσει το mining ή θα έρθει πιο κοντά στην απάντηση του αριθμητικού προβλήματος θα πάρει τα tokens. Αυτός ο τρόπος mining ονομάζεται proof of work. Στο μαθηματικό πρόβλημα δεν εμπλέκονται όντως προηγμένα μαθηματικά και υπολογισμοί. Αυτό που στην πραγματικότητα κάνουν οι υπολογιστές είναι να προσπαθούν να μαντέψουν πρώτοι έναν δεκαεξαδικό αριθμό (“hash”) με 64 ψηφία που είναι μικρότερος ή ίσος με το αποτέλεσμα.

Το κακό με αυτήν την μέθοδο είναι ότι είναι θέμα “τύχης” και είναι μια πολύ χρονοβόρα και δύσκολη δουλειά καθώς ο αριθμός είναι ανάμεσα σε τρισεκατομμύρια άλλους αριθμούς. Όσο περισσότεροι είναι οι εξορύκτες τόσο πιο δύσκολο είναι να βρεθεί ο τυχαίος αριθμός. Αυτό είναι γνωστό και ως mining difficulty(το είχαμε δει περιληπτικά στην ενότητα «Τι είναι το Blockchain»). Για να γίνει mining ενός μπλοκ, οι miners χρειάζονται πολύ μεγάλη υπολογιστική δύναμη. Όσο μεγαλύτερο είναι το hash rate ενός miner, τόσο μεγαλύτερες πιθανότητες έχει να βρει την λύση πρώτος.

Το mining εκτός από την αμοιβή που δίνει στον επενδυτή και την υποστήριξη του οικοσυστήματος του Bitcoin, είναι και ο τρόπος που νέα μπλοκ εισχωρούνται στο blockchain. Για παράδειγμα, τον Σεπτέμβρη του 2021 υπήρχαν περίπου 18.21 εκατομμύρια bitcoins και τα συνολικά bitcoins που θα παραχθούν ποτέ, είναι 21 εκατομμύρια. Εκτός από το μπλοκ της γέννησης, το πρώτο μπλοκ που δημιουργήθηκε χάρη στον/στους Satoshi Nakamoto, τα υπόλοιπα μπλοκ δημιουργήθηκαν με την μέθοδο του mining.

Πέρα από το μερίδιο που παίρνουν οι εξορύκτες bitcoin, έχουν και το δικαίωμα της ψήφου, ανάλογα με το ποσό του bitcoin που διαθέτουν όταν προταθεί μια αλλαγή στο πρωτόκολλο του δικτύου του bitcoin, αυτό είναι γνωστό ως BIP(Bitcoin Improvement Protocol). Δηλαδή οι miners μπορούν να πάρουν αποφάσεις σε θέματα πάνω στο bitcoin όπως ένα νέο fork.

Οι ανταμοιβές για την εξόρυξη bitcoin μειώνονται κατά το ήμισυ κάθε 4 χρόνια, όπως μειώνεται και το σύνολο του bitcoin. Όταν το bitcoin εξορύχθηκε για πρώτη φορά το 2009, η ανταμοιβή του ήταν 50 BTC. Το 2012 μειώθηκε στο ήμισυ, δηλαδή στα 25 BTC και το 2016 κατέβηκε στα 12,5 μέχρι τις 6 Μαΐου που η ανταμοιβή του είχε πέσει στα 6,25 BTC. Τον Σεπτέμβρη του 2021 η τιμή του bitcoin ήταν 45,000 δολάρια δηλαδή ο εξορύκτης θα κέρδιζε 281,250(6,25 x 45,000) δολάρια πράγμα που δεν το κάνει τόσο δαπανηρό.

Για να μπορέσει να παρακολουθήσει κανείς πότε θα πραγματοποιηθούν τα halvings, μπορεί να δει το bitcoin clock, το οποίο ενημερώνεται σε πραγματικό χρόνο. Ενδιαφέρον είναι ότι η τιμή του bitcoin, τείνει να αντιστοιχεί με την μείωση των νέων κρυπτονομισμάτων που υπάρχουν στην αγορά. Αυτός ο μειωμένος ρυθμός πληθωρισμού αύξησε τη σπανιότητα και ιστορικά η τιμή αυξήθηκε μαζί του.

Αν και στην αρχή του bitcoin, μεμονωμένα άτομα ήταν δυνατόν να ανταγωνιστούν για τα μπλοκ χρησιμοποιώντας τον προσωπικό τους υπολογιστή από το σπίτι, αυτό δεν ισχύει πλέων καθώς το ρεύμα που πρέπει να παραχθεί, είναι ακριβότερο από τα κέρδη που μπορεί να υπάρξουν. Ο κυριότερος λόγος για αυτό είναι ότι η δυσκολία αλλάζει με την πάροδο του χρόνου και με το πλήθος των ατόμων που κάνουν mining.

Προκειμένου να διασφαλιστεί η ομαλή λειτουργία του blockchain και η ικανότητά του να επεξεργάζεται και να επαληθεύει συναλλαγές, το Bitcoin προσπαθεί να παράγει ένα μπλοκ κάθε 10 λεπτά. Παρόλα αυτά αν λειτουργούν 10 εκατομμύρια υπολογιστές προκειμένου να κάνουν εξόρυξη ένα μπλοκ, θα φτάσουν στην λύση γρηγορότερα από ότι αν οι υπολογιστές

ήταν λιγότεροι. Για αυτόν τον λόγο το Bitcoin έχει σχεδιαστεί ώστε να προσαρμόζει και να αλλάζει το επίπεδο δυσκολίας κάθε 2016 μποκ ή κάθε 2 εβδομάδες.

Όσο πιο πολύ επεξεργαστική δύναμη υπάρχει για την δημιουργία ενός μπλοκ, τόσο πιο πολύ αυξάνεται και η δυσκολία του προβλήματος, έτσι ώστε να υπάρχει μια σταθερή δημιουργία μποκ. Λιγότερη επεξεργαστική δύναμη σημαίνει ότι το επίπεδο δυσκολίας γίνεται πιο εύκολο. Με το σημερινό επίπεδο δυσκολίας, ένας προσωπικός υπολογιστής δεν θα φτάσει καν κοντά στην λύση του προβλήματος.

Όλα αυτά σημαίνουν ότι για να γίνει η εξόρυξη ανταγωνιστική θα πρέπει οι εξορύκτες να επενδύσουν σε ισχυρές κάρτες γραφικών, φάρμες υπολογιστών καθώς και ASIC(application specific integrated circuit) τα οποία κοστίζουν από 500 ευρώ μέχρι και δεκάδες χιλιάδες ευρώ. Πολλοί που κάνουν εξόρυξη στο Ethereum, αγοράζουν και συνδυάζουν μεμονωμένες κάρτες γραφικών(GPU) σαν έναν τρόπο στην προσπάθειά τους να μειωθούν τα έξοδα τους.

Για να δώσουμε ένα παράδειγμα mining ας υποθέσουμε ότι λέμε σε τρεις φίλους να μαντέψουν έναν αριθμό από το 1 μέχρι το 100 ο οποίος είναι σφραγισμένος σε έναν κλειστό φάκελο. Οι εξορύκτες στο παράδειγμα δεν χρειάζεται να μαντέψουν ακριβώς τον αριθμό και μπορούν να προσπαθήσουν όσες φορές θέλουν αρκεί ο αριθμός να είναι ίσος ή μικρότερος από τον αριθμό μας.

Ας υποθέσουμε ότι ο φάκελος έχει τον αριθμό 19. Αν ο Α φίλος υποθέσει ότι ο αριθμός είναι ο 21, έχει χάσει ενώ αν ο Β φίλος και ο Γ φίλος υποθέσουν ότι ο αριθμός είναι ο 16 και ο 12 αντίστοιχα, είναι και οι 2 απαντήσεις δεκτές διότι είναι μικρότεροι αριθμοί από τον αριθμό που έχω στον φάκελο. Αν ο φίλος Β και Γ απαντήσουν ταυτόχρονα, τότε η αναλογία καταρρέει. Αν οι φίλοι μου όμως ήταν εκατομμύρια και ο αριθμός που ζητούσα ήταν ένας αριθμός δεκαεξαδικός με 64 ψηφία, βλέπουμε πως το πρόβλημα γίνεται πολύ πιο δύσκολο.

Στο δίκτυο του Bitcoin, ταυτόχρονες σωστές απαντήσεις μπορούν να υπάρξουν και υπάρχουν συχνά, αλλά μόνο ένας μπορεί να ανταμειφθεί. Αν υπάρχουν 2 ή παραπάνω “νικητές”, το δίκτυο του Bitcoin θα ψηφήσει ποιος θα ανταμειφθεί από τους νικητές με ποσοστό 51% ή παραπάνω.

Συνήθως ο εξορύκτης που ανταμείβεται είναι αυτός που έχει κάνει την περισσότερη δουλειά και επαλήθευσε τις περισσότερες συναλλαγές. Το μπλοκ που έχασε, ονομάζεται “orphan block”, τα οποία μπλοκ είναι αυτά που δεν προστίθενται στο blockchain. Οι εξορύκτες που βρήκαν το μυστικό hash αλλά δεν έχουν επαληθεύσει συναλλαγές στο blockchain, δεν παίρνουν την ανταμοιβή. Η εξόρυξη(mining) μπορεί να γίνει με μια από τις παρακάτω κατηγορίες, ανάλογα, ποια από αυτές είναι δεκτή στο δίκτυο που είναι επιθυμητό να γίνει η εξόρυξη. [44]

3.1.1. Proof of Work

Το πρωτόκολλο proof of work είναι ο τρόπος εξόρυξης που χρησιμοποιούν διάφορα κρυπτονομίσματα όπως είναι το bitcoin και το Ethereum. Το proof of work περιγράφει ένα

σύστημα το οποίο απαιτεί μεγάλες ποσότητες ενέργειας και προσπάθειας προκειμένου να αποτραπούν κακοήθεις χρήσεις υπολογιστικής ισχύος(π.χ. αποστολή spam e-mail, Dos attacks κ.α.). Ο Hal Finney ήταν ο πρώτος που συνδύασε το proof of work με τα κρυπτονομίσματα φέρνοντας το 2004 την ιδέα της εξόρυξης χρησιμοποιώντας τον αλγόριθμο κατακερματισμού SHA-256.

Μετά την εισαγωγή του το 2009, το bitcoin ήταν το πρώτο κρυπτονόμισμα που χρησιμοποίησε τον αλγόριθμο proof of work για την εξόρυξη BTC(ο Finney ήταν ο παραλήπτης στην πρώτη συναλλαγή που έγινε στον κόσμο). Το proof of work εντάχθηκε και σε άλλα πολλά κρυπτονομίσματα επιτρέποντας ασφαλές και αποκεντρωμένες συναλλαγές.

Το bitcoin είναι ένα ψηφιακό νόμισμα που υποστηρίζεται από το blockchain, στο οποίο περιέχονται καταγραφές από όλες τις συναλλαγές bitcoin, τοποθετημένες σε διαδοχικά μπλοκ, έτσι ώστε να μην μπορούν οι χρήστες να ξοδέψουν παραπάνω ή λιγότερο από όσο έχει συμφωνηθεί. Προκειμένου να αποφεύγονται οι παραβιάσεις, το blockchain είναι ανοιχτό στο κοινό, και μια τροποποιημένη έκδοσή του θα απορρίπτονταν από τους χρήστες του.

Ο τρόπος με τον οποίο οι χρήστες εντοπίζουν παραβιάσεις γίνεται μέσω των κατακερματισμών(hashes) που είναι δεαεξαδικοί αριθμοί αποτελούμενοι από 64 ψηφία, οι οποίοι χρησιμεύουν στην απόδειξη εργασίας(Proof of Work), τοποθετώντας ένα σύνολο δεδομένων μέσω μιας συνάρτησης κατακερματισμού και θα πρέπει να δημιουργηθεί μόνο ένας κατακερματισμός.

Λόγο του φαινομένου “avalanche effect” αν αλλαχθεί έστω και 1 bit από τα αρχικά δεδομένα, θα αλλάξει όλο το τελικό αποτέλεσμα. Ότι μέγεθος και να έχει το αρχικό σύνολο δεδομένων, ο κατακερματισμός που δημιουργήθηκε θα έχει το ίδιο μήκος. Ο κατακερματισμός είναι μονόδρομος, δηλαδή δεν μπορεί να χρησιμοποιηθεί για να δημιουργηθούν τα αρχικά δεδομένα, μόνο για να γίνει η επαλήθευση ότι τα τελικά δεδομένα ταιριάζουν με τα αρχικά.

Η δημιουργία οποιουδήποτε κατακερματισμού για ένα σύνολο συναλλαγών από bitcoin χρησιμοποιώντας έναν σύγχρονο υπολογιστή, θα ήταν ανούσιο, οπότε προκειμένου να προχωρήσει η εργασία, το δίκτυο Bitcoin θέτει μια συγκεκριμένη δυσκολία. Η δυσκολία προσαρμόζεται έτσι ώστε ένα καινούργιο μπλοκ να εξορύσεται και να προστίθεται στην λίστα των μπλοκ κάθε 10 λεπτά. Η δυσκολία μπορεί να προσαρμοστεί, θέτοντας έναν στόχο για τον κατακερματισμό: όσο μικρότερος είναι ο αριθμός, τόσο μικρότερο είναι το σύνολο των κατακερματισμών και τόσο πιο δύσκολη είναι η δημιουργία του. Στην πράξη, αυτό σημαίνει ότι ο κατακερματισμός ξεκινάει από πολλά μηδενικά.

Εφόσον με μια συλλογή δεδομένων μπορεί να παραχθεί μόνο ένας συγκεκριμένος κατακερματισμός, οι εξορύκτες αλλάζουν την αρχική μεταβλητή που ονομάζεται nonce(number used once). Όταν βρεθεί ένας έγκυρος κατακερματισμός, μεταδίδεται στο δίκτυο και δημιουργείται το καινούργιο μπλοκ.

Η εξόρυξη είναι ένας αγώνας μεταξύ υπολογιστών αλλά μοιάζει με μια τυχαία κλήρωση. Κατά μέσο όρο ολοκληρώνεται μια εξόρυξη κάθε 10 λεπτά, αλλά δεν μπορεί να ξέρει κανείς ποιος κέρδισε. Οι εξορύκτες συνήθως συγκεντρώνονται για να αυξήσουν τις πιθανότητες να κάνουν επιτυχείς εξορύξεις το οποίο δημιουργεί χρεώσεις συναλλαγών, οι οποίες επιβραβεύονται με BTC και δημιουργείτε και ένα καινούργιο μπλοκ στο blockchain.

Το proof of work καθιστά εξαιρετικά δύσκολη την αλλαγή οποιασδήποτε πτυχής του blockchain, καθώς μια τέτοια αλλαγή θα απαιτούσε να ξαναγίνουν οι εξορύξεις των επόμενων μπλοκ. Κάνει επίσης πολύ δύσκολο στους χρήστες ή στα γκρουπ ανθρώπων, να μονοπωλούν την υπολογιστική ισχύει του δικτύου, λόγο του ότι οι μηχανές που χρειάζονται έχουν πολύ μεγάλη αξία.

Το proof of work χρειάζεται από έναν υπολογιστή, να συμμετέχει σε τυχαίες λειτουργείες κατακερματισμού, έως ότου η έξοδος του να είναι ίση ή μικρότερη με το σωστό ελάχιστο ποσό μηδενικών στην αρχή. Για παράδειγμα στις 4 Δεκεμβρίου του 2020, ο κατακερματισμός για το μπλοκ 660,000, ήταν ο αριθμός 000000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6 και η ανταμοιβή για αυτό το μπλοκ ήταν 6,25 BTC.

Το συγκεκριμένο μπλοκ θα περιέχει για πάντα 745 συναλλαγές με περίπου 1,666 bitcoins, καθώς και το hash του προηγούμενου μπλοκ. Εάν κάποιος προσπαθούσε να αλλάξει οποιοδήποτε ποσό συναλλαγής, ακόμη και κατά 0,000001 bitcoin, ο κατακερματισμός που θα προέκυπτε θα ήταν μη αναγνωρίσιμος και το δίκτυο θα απέρριπτε αυτήν την απόπειρα απάτης.

Το proof of work απαιτεί τους κόμβους ενός δικτύου για να παρέχει την απόδειξη ότι μια συγκεκριμένη υπολογιστική ισχύ έχει ξοδευτεί, προκειμένου να επιτευχθεί συναίνεση με έναν αποκεντρωμένο τρόπο ώστε να μην μπορέσουν να εισέρθουν στο δίκτυο και να αποκλειστούν τα κακοήθη άτομα.

Το ίδιο το έργο(proof of *work*) είναι αυθαίρετο. Το bitcoin, περιλαμβάνει επαναλήψεις των αλγορίθμων κατακερματισμού SHA-256. Ο νικητής ενός μπλοκ, συγκεντρώνει και καταγράφει τις συναλλαγές από ένα mempool, στο επόμενο μπλοκ. Επειδή ο νικητής διαλέγεται τυχαία, ανάλογα με το πόσο έχει “εργαστεί”, προωθεί τους υπόλοιπους στο δίκτυο να είναι ειλικρινείς μεταξύ τους και να καταγράφουν μόνο τις σωστές συναλλαγές.

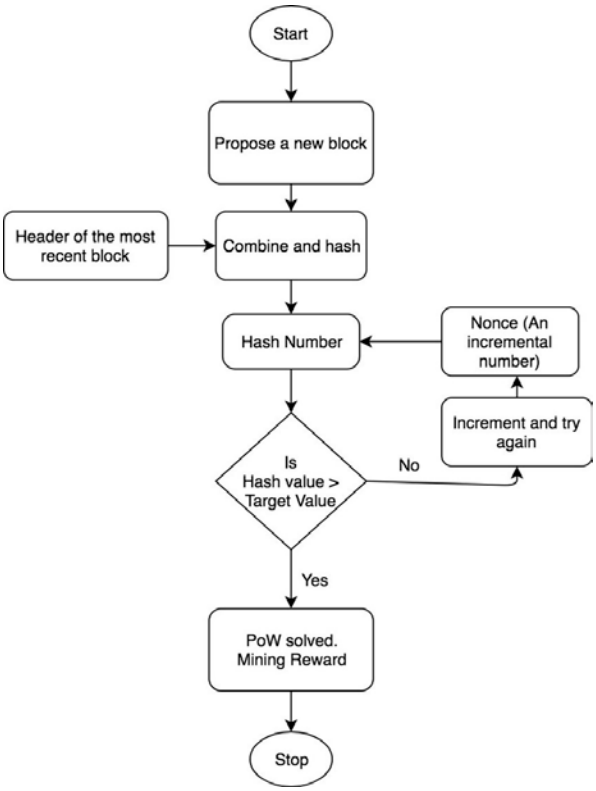
Επειδή είναι αποκεντρωμένοι και έχουν σχεδιαστεί σαν ένα peer-to-peer δίκτυο, τα blockchain, όπως τα δίκτυα κρυπτονομισμάτων, απαιτούν έναν τρόπο για την επίτευξη ασφάλειας και συναίνεσης. Το proof of work είναι μια τέτοια μέθοδος που καθιστά τρομερά ταλαίπωρη να προσπαθήσει κάποιος να καταλάβει όλο το δίκτυο. Υπάρχουν και άλλοι μηχανισμοί απόδειξης οι οποίοι απαιτούν λιγότερους πόρους όπως είναι το Proof of Stake(PoS), το Proof of History(PoH) και το Proof of Burn(PoB), τους οποίους θα τους αναλύσουμε παρακάτω. Χωρίς κάποιον μηχανισμό απόδειξης, το δίκτυο και τα δεδομένα που είναι αποθηκευμένα, είναι ευάλωτα σε επιθέσεις.

Το Bitcoin χρησιμοποιεί έναν αλγόριθμο proof of work, βασισμένο στον αλγόριθμο SHA-256, για την επικύρωση και την επιβεβαίωση συναλλαγών, καθώς και για την δημιουργία καινούργιων bitcoin.

Το proof of stake είναι ένας μηχανισμός συναίνεσης που επιλέγει τυχαία τον κόμβο για εξόρυξη ή για να επικυρώσει συναλλαγές μπλοκ, ανάλογα με τον αριθμό των νομισμάτων που κατέχει αυτός ο κόμβος. Όσο περισσότερα tokens βρίσκονται σε ένα πορτοφόλι, τόσο περισσότερη δύναμη εξόρυξης παρέχεται σε αυτό. Ενώ ο μηχανισμός proof of stake χρειάζεται σημαντικά λιγότερους πόρους για τις εξορύξεις, έχει άλλα ελαττώματά, συμπεριλαμβανομένου και της μεγαλύτερης πιθανότητας επίθεσης του 51% σε μικρότερα altcoins καθώς και του κινήτρου να έχει κάποιος tokens και να μην τα χρησιμοποιεί.

Το Proof of Work (PoW) απαιτεί τεράστια ποσά κατανάλωσης ενέργειας για να τροφοδοτήσει την υπολογιστική ισχύ. Το Proof of Stake (PoS) δίνει ισχύ εξόρυξης με βάση το ποσοστό των νομισμάτων που κατέχει ένας εξορύκτης.

Με το Proof of Stake (PoS), οι εξορύκτες κρυπτονομισμάτων μπορούν να εξορύσσουν ή να επικυρώσουν νέα μπλοκ συναλλαγών με βάση το ποσό των νομισμάτων που κατέχει ο εξορύκτης. [15]



Εικόνα 7: Διάγραμμα παραδείγματος Proof of Work(PoW)[38]

3.1.2. Proof of Stake

Η έννοια του Proof of Stake (PoS) δηλώνει ότι ένα άτομο μπορεί να εξορύξει ή να επικυρώσει συναλλαγές μπλοκ ανάλογα με τον αριθμό των νομισμάτων που κατέχει. Αυτό σημαίνει ότι όσα περισσότερα νομίσματα κατέχει ένας miner, τόσο περισσότερη δύναμη εξόρυξης έχει. Το Proof of Stake (PoS) δημιουργήθηκε ως εναλλακτική του Proof of Work (PoW), που είναι ο αρχικός αλγόριθμος συναίνεσης στην τεχνολογία Blockchain και χρησιμοποιείται για την επιβεβαίωση συναλλαγών και την προσθήκη νέων μπλοκ στην αλυσίδα.

Το Proof of Stake (POS) θεωρείται λιγότερο επικίνδυνο όσον αφορά τη δυνατότητα επίθεσης στο δίκτυο, καθώς δομεί την αποζημίωση με τέτοιο τρόπο που καθιστά μια επίθεση λιγότερο συμφέρουσα.

Το Proof of Work (PoW) απαιτεί από κάθε κόμβο στο δίκτυο του Bitcoin, να λύσει ένα πρόβλημα. Ο πρώτος κόμβος που θα το λύσει, του δίνεται το δικαίωμα να παρέχει ένα νέο μπλοκ στο δίκτυο καθώς και ένα ποσό των token. Οι κόμβοι είναι το σώμα του blockchain και επαληθεύουν την ακεραιότητα των συναλλαγών σε κάθε μπλοκ. Όταν επαληθευτεί ένα μπλοκ συναλλαγών, γράφεται στην λίστα των υπολοίπων μπλοκ στο blockchain.

Το πρωτόκολλο Proof of Stake(PoS) δημιουργήθηκε σαν ένας εναλλακτικός αλγόριθμος που προσπαθεί να αντιμετωπίσει τις ανησυχίες που υπάρχουν περί της επεκτασιμότητα και του περιβάλλοντος που έχει το πρωτόκολλο Proof of Work(PoW).

Οι εξορύξεις απαιτούν τεράστια υπολογιστική ισχύ για να εκτελέσουν διαφορετικούς κρυπτογραφικούς αλγόριθμους και να “ξεκλειδωθούν” καινούργιες υπολογιστικές προκλήσεις. Αυτή η υπολογιστική ισχύ μεταφράζεται σε μεγάλες ποσότητες ηλεκτρικού ρεύματος που απαιτείται στο πρωτόκολλο Proof of Work(PoW).

Το 2015, υπολογιζόταν ότι για να παραχθεί ένα bitcoin, χρειαζόταν η ίδια ποσότητα ρεύματος που χρησιμοποιούσαν 1.57 νοικοκυριά καθημερινά στην Αμερική. Σύμφωνα με το Bitcoin Electricity Consumption Index του πανεπιστημίου του Cambridge, ξοδεύονταν περίπου 119,87 terawatt ανά ώρα τον χρόνο για την παραγωγή bitcoin, το οποίο είναι περισσότερο ρεύμα από ότι χώρες όπως τα Ενωμένα Αραβικά Εμιράτα και η Ολλανδία καταναλώνουν ετησίως. Για να πληρώσουν το ρεύμα που καταναλώθηκε, οι εξορύκτες συνήθως πωλούσαν τα κρυπτονομίσματα που κέρδιζαν, πράγμα που μείωνε την αξία του κρυπτονομίσματος.

Το πρωτόκολλο PoW θεωρείτε από πολλούς ασταθείς, καθώς η κατανάλωση ενέργειας που απαιτείται για να παραχθεί ένα bitcoin, δημιουργεί μεγάλες ποσότητες ηλεκτρικών απόβλητων, κυρίως επειδή οι μηχανές ASIC που χρησιμοποιούνται για την εξόρυξη bitcoin, δεν έχουν κάποια άλλη χρησιμότητα.

Το Bitcoin Energy Consumption Index, υπολογίζει ότι το δίκτυο του Bitcoin καταναλώνει 132,5 terawatts ανά ώρα ετησίως μέχρι την ημέρα της 29^{ης} Ιουνίου 2021. Το Bitcoin Energy Consumption Index δηλώνει επίσης ότι για να παραχθεί ένα bitcoin την χρονιά του 2021,

πρέπει να καταναλωθεί περισσότερη ενέργεια από όσο καταναλώνει ένα μέσο νοικοκυριό της Αμερικής σε περίπου 57.3 ημέρες, ο οποίος αριθμός είναι πολύ παραπάνω από τον αριθμό του 2015 όπου ήταν μόλις 1,57 ημέρες ενός μέσου Αμερικάνικου νοικοκυριού. Οι εξορύκτες bitcoin συχνά πληρώνουν την ζημία που προήλθε από την εξόρυξη μέσω των κερδών τους. Ως αποτέλεσμα, οι εξορύκτες επηρεάζουν άμεσα την τιμή των κρυπτονομισμάτων.

Σύμφωνα με μια μελέτη του Ιουνίου 2021, οι απαιτήσεις του Bitcoin δικτύου έχουν αυξηθεί επειδή η τιμή του bitcoin έχει αυξηθεί και η ίδια όσο ποτέ πριν. Οι τιμές αύξησαν τις συμμετοχές των εξορυκτών bitcoin, δίνοντας τους το κίνητρο για να ξοδέψουν ώστε να κάνουν εξορύξεις εφόσον η τιμή του bitcoin ήταν τόσο μεγάλη.

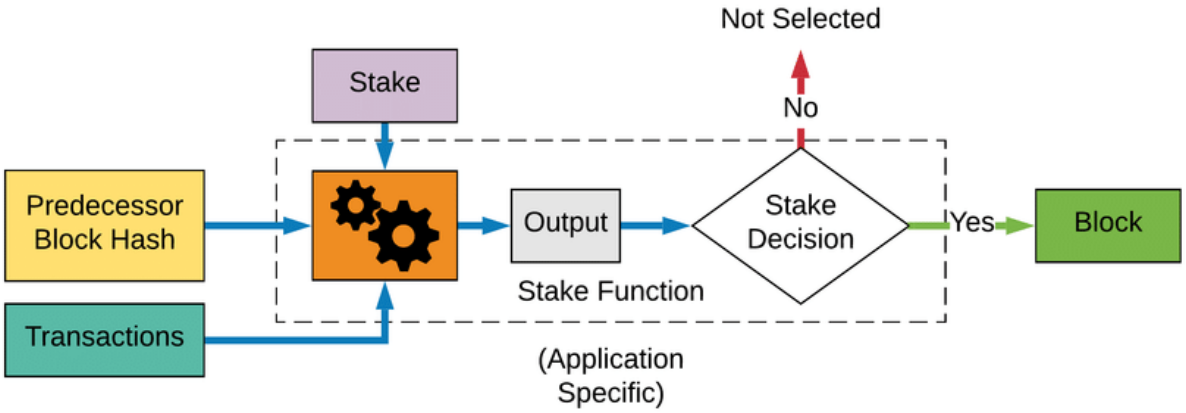
Ο αλγόριθμος του Proof of Stake επιδιώκει να λύσει αυτό το πρόβλημα αντικαθιστώντας το staking έναντι της υπολογιστικής ισχύς, όπου η ισχύ εξόρυξης ενός ατόμου περιορίζεται από το ποσό κρυπτονομισμάτων που έχει στην κατοχή του. Αυτό σημαίνει τεράστια μείωση στην κατανάλωση ενέργειας και οι συσκευές μιας χρήσης όπως οι μηχανές ASIC δεν είναι πλέον αναγκαίες για τις εξορύξεις.

Με αυτόν τον τρόπο, το Proof of Stake(PoS) αντί να χρησιμοποιεί ενέργεια για να μαντεύει την σωστή απάντηση ενός γρίφου, ο εξορύκτης περιορίζεται στην εξόρυξη ενός ποσοστού συναλλαγών που αντικατοπτρίζει το μερίδιο ιδιοκτησίας του. Για παράδειγμα, ένας εξορύκτης που κατέχει το 3% των διαθέσιμων νομισμάτων μπορεί θεωρητικά να εξορύξει μόνο το 3% των μπλοκ. Το πρώτο κρυπτονόμισμα που υιοθέτησε τη μέθοδο PoS ήταν το Peercoin. Το Nxt, το Blackcoin και το ShadowCoin ακολούθησαν σύντομα το παράδειγμά του.

Το Bitcoin χρησιμοποιεί ένα σύστημα PoW και αυτό το κάνει ευάλωτο σε μια πιθανή Τραγωδία των Κοινών. Η Τραγωδία των Κοινών αναφέρεται σε ένα μελλοντικό χρονικό σημείο όπου θα υπάρχουν λιγότεροι διαθέσιμοι εξορύκτες bitcoin λόγω της μικρής έως καθόλου ανταμοιβής από την εξόρυξη. Οι μόνες χρεώσεις που θα κερδηθούν θα προέρχονται από τις χρεώσεις συναλλαγών οι οποίες επίσης θα μειωθούν με την πάροδο του χρόνου καθώς οι χρήστες θα επιλέγουν να πληρώνουν χαμηλότερες χρεώσεις για τις συναλλαγές τους.

Με το Proof of Work (PoW), κάποιος εισβολέας θα πρέπει να αποκτήσει το 51% του κρυπτονομίσματος για να καταφέρει μια επίθεση. Το Proof of Stake(PoS) αποφεύγει κάτι τέτοιο, κάνοντάς το μειονεκτικό για κάποιον εξορύκτη με 51% του κρυπτονομίσματος να φέρει εις πέρας μια τέτοια επίθεση. Αν και θα ήταν δαπανηρό και χρονοβόρο να έχει κανείς το 51% ενός έμπιστου κρυπτονομίσματος, δεν θα τον σύμφερε καθόλου να φέρει εις πέρας μια επίθεση στο δίκτυο.

Εάν η αξία του κρυπτονομίσματος πέσει, αυτό σημαίνει ότι και η αξία των κρυπτονομισμάτων θα πέσει επίσης, και έτσι ο ιδιοκτήτης με τα περισσότερα κρυπτονομίσματα θα έχει μεγαλύτερο κίνητρο για τη διατήρηση ενός ασφαλούς δικτύου. [16]



Εικόνα 8: Διάγραμμα παραδείγματος Proof of Stake(PoS)[39]

3.1.3. Proof of History

Αντί να υπάρχει εμπιστοσύνη στην χρονική σήμανση σε μια συναλλαγή, μπορούμε να αποδείξουμε ότι η συναλλαγή πραγματοποιήθηκε μεταξύ δύο άλλων συμβάντων. Ο αλγόριθμος Proof of History(PoH) είναι ένα τέτοιο πρωτόκολλο και είναι μια συχνή και επαληθεύσιμη συνάρτηση καθυστέρησης. Μια επαληθεύσιμη συνάρτηση καθυστέρησης έχει έναν συγκεκριμένο αριθμό διαδοχικών βημάτων για να αξιολογήσει και να παράγει ένα μοναδικό αποτέλεσμα το οποίο είναι επαληθεύσιμο και δημόσιο στον καθένα.

Το Proof of History(PoH) είναι μια ακολουθία υπολογισμών οι οποίοι παρέχουν έναν τρόπο κρυπτογραφικής επαλήθευσης ανάμεσα σε δύο συμβάντα. Χρησιμοποιούν μια κρυπτογραφικά ασφαλή συνάρτηση, γραμμένη, έτσι ώστε το αποτέλεσμα να μην μπορεί να παραχθεί τυχαία με βάση την είσοδο αλλά να πρέπει να ολοκληρωθεί μια διαδικασία για να παραχθεί το αποτέλεσμα.

Η συνάρτηση εκτελείται με μια σειρά μέσα σε έναν πυρήνα, του οποίου η προηγούμενη έξοδός του είναι η τρέχουσα είσοδος καθώς και περιοδικά καταγράφεται η τρέχουσα έξοδος αλλά και πόσες φορές έχει κληθεί. Η έξοδος μπορεί στην συνέχεια να κληθεί εκ νέου και να επαληθευτεί από άλλους υπολογιστές παράλληλα, ελέγχοντας κάθε τμήμα ακολουθίας σε ξεχωριστό πυρήνα.

Τα δεδομένα μπορούν να αποκτήσουν την δική τους χρονοσφραγίδα μέσα στην ακολουθία προσθέτοντας τα δεδομένα(ή έναν κατακερματισμό των δεδομένων) στην κατάσταση της συνάρτησης. Η καταγραφή της κατάστασης, του ευρετηρίου και των δεδομένων, μπορεί να διασφαλίσει ότι τα δεδομένα δημιουργήθηκαν πριν ο επόμενος κατακερματισμός είχε δημιουργηθεί στην ακολουθία. Αυτός ο σχεδιασμός, υποστηρίζει οριζόντια κλιμάκωση, καθώς πολλαπλές γεννήτριες συγχρονίζονται μεταξύ τους αναμιγνύοντας την κατάστασή τους σε άλλες ακολουθίες.

Το σύστημα, σχεδιάστηκε για να λειτουργεί ως εξής: Με μια κρυπτογραφική συνάρτηση κατακερματισμού, του οποίου η έξοδος δεν μπορεί να μαντευθεί χωρίς να εκτελεστεί η συνάρτηση(π.χ. SHA-256, ripemd, κ.α.), τρέχει την συνάρτηση με μια τυχαία αρχική τιμή και παίρνει το αποτέλεσμα και το προσθέτει ως την αρχική τιμή της ίδιας της συνάρτησης, καταγράφοντας το πόσες φορές κλήθηκε η συνάρτηση μαζί με το τελικό αποτέλεσμά της.

Παραδείγματος χάρη: Ο αλγόριθμος Proof of History τρέχει και ο κατακερματισμός ακολουθίας 1 βγάζει με τον αλγόριθμο SHA-256, τον αριθμό 1, ο κατακερματισμός ακολουθίας 2 παίρνοντας σαν είσοδο το αποτέλεσμα του προηγούμενου κατακερματισμού(1) βγάζει με τον ίδιο αλγόριθμο τον αριθμό 2, ο κατακερματισμός ακολουθίας 3 παίρνοντας το αποτέλεσμα του προηγούμενου κατακερματισμού, βγάζει αποτέλεσμα τον αριθμό 3, κ.ο.κ..

Όσο η επιλεγμένη κατακερματισμένη συνάρτηση είναι ανθεκτική, το σύνολο κατακερματισμών μπορεί να υπολογιστεί με ένα thread του επεξεργαστή. Αυτό προκύπτει επειδή δεν μπορεί να προβλεφθεί για παράδειγμα ο εν συνέχεια κατακερματισμός, χωρίς να έχουν υπολογιστεί οι 300 προηγούμενοι κατακερματισμοί με τον τυχαίο αρχικό αριθμό. Έτσι μπορούμε να υπολογίσουμε τον χρόνο μεταξύ του αρχικού κατακερματισμού και του τριακοσιοστού.

Μπορούμε να δούμε με το Proof of History(PoH) πόσο σημαντικά λιγότεροι πόροι ενέργειας χρειάζονται συγκριτικά με το Proof of Work(PoW). Αυτή την στιγμή, το Proof of History(PoH) χρησιμοποιείται από το κρυπτονόμισμα Solana. [17]

3.1.4. Proof of Burn

Το Proof of Burn(PoB) είναι ένας από τους πολλούς μηχανικούς αλγόριθμους και εφαρμόζεται στο δίκτυο του blockchain για να διαβεβαιώσει ότι όλοι οι συμμετέχοντες κόμβοι συμφωνούν σχετικά με την πραγματική και έγκυρη κατάσταση του δικτύου του blockchain. Ο αλγόριθμος είναι ενσωματωμένος για να αποφεύγεται ένα κρυπτονόμισμα να χρησιμοποιηθεί για παραπάνω από μια φορά.

Το Proof of Burn, ακολουθεί την αρχή της “καύσης” των κρυπτονομισμάτων που έχουν στην κατοχή τους οι εξορύκτες και τους παρέχουν το δικαίωμα της εξόρυξης. Τα κρυπτονομίσματα χρησιμοποιούν διάφορες μεθόδους για να επικυρώσουν τα δεδομένα που βρίσκονται στα blockchain, συμπεριλαμβανομένου και της Proof of Burn(PoB).

Το Proof of Burn(PoB) αποτελεί την τρίτη προσπάθεια για την δημιουργία ενός συστήματος για την αποτροπή των κακόβουλων δραστηριοτήτων και βελτιώνει παράλληλα την λειτουργία του blockchain. Το Proof of Burn(PoB) και το Proof of Stake(PoS) είναι και οι δύο μέθοδοι οι οποίες υπάρχουν για την πρόληψη κακόβουλων ατόμων μέσα στα blockchain.

Το blockchain είναι η κύρια βάση δεδομένων ενός κρυπτονομίσματος. Κατέχει όλες τις πληροφορίες για τις μεταφορές/συναλλαγές στα μπλοκ τα οποία δρουν σαν μονάδες αποθηκευτικών δεδομένων. Ένα μπλοκ γράφεται μόνο όταν οι κόμβοι του blockchain συμφωνούν πως το μπλοκ είναι αληθές. Λόγο της αποκεντρωμένης φύσης του δικτύου του Blockchain, χρειάζεται ένας αυτοματοποιημένος μηχανισμός για να διαβεβαιώνει πως όλοι οι συμμετέχοντες κόμβοι, συμφωνούν μεταξύ τους.

Το Proof of Burn(PoB) είναι ένας εναλλακτικός αλγόριθμος που προσπαθεί να αντιμετωπίσει το ζήτημα της υπερ-κατανάλωσης της ενέργειας. Το PoB συνήθως αποκαλείται ένα σύστημα POW χωρίς την κατανάλωσης ενέργειας. Λειτουργεί με την αρχή ότι επιτρέπει στους εξορύκτες να “κάψουν” τα ψηφιακά τους νομίσματα. Έπειτα τους επιτρέπεται να γράφουν μπλοκ ανάλογα με το ποσό των κρυπτονομισμάτων που “έκαψαν”.

Ο Iain Steward, ο ιδρυτής του μηχανισμού Proof of Burn(PoB), χρησιμοποιεί την αναλογία για να περιγράψει τον αλγόριθμο: τα “καμένα” νομίσματα είναι σαν εξέδρες εξόρυξης. Στην αναλογία αυτή, ένας εξορύκτης, “καίει” τα νομίσματά του για να αγοράσει εξέδρες εξόρυξης που τον επιτρέπουν να εξορύξει μπλοκ. Όσο περισσότερα νομίσματα “καίγονται” από τον εξορύκτη, τόσο περισσότερο θα μπορεί να εξορύξει.

Για να γίνει η “καύση” των νομισμάτων, οι εξορύκτες τα στέλνουν σε μια διεύθυνση στο blockchain, η οποία δεν υπάρχει. Αυτός ο τρόπος δεν καταναλώνει πολλούς πόρους πέρα των “καμένων” νομισμάτων και διασφαλίζει ότι το δίκτυο παραμένει ενεργό. Ανάλογα με την εφαρμογή, οι εξορύκτες επιτρέπεται να “κάψουνε” το ίδιο το κρυπτονόμισμα ή ένα άλλο κρυπτονόμισμα που κατέχουν μέσα στο blockchain. Σε αντάλλαγμα, τους δίνεται το ίδιο το νόμισμα μέσα στο blockchain.

Μπορεί κανείς να “κάψει” και να εξορύξει πάνω στο μπλοκ ενός άλλου, ο οποίος μπορεί έπειτα να πάρει τις συναλλαγές και να τις προσθέσει στο μπλοκ του. Ουσιαστικά, όλη αυτή η δραστηριότητα της “καύσης”, κρατάει το δίκτυο ενεργό και όλοι οι συμμετέχοντες βραβεύονται για τις δραστηριότητές τους(της “καύσης” των δικών τους νομισμάτων και των άλλων).

Για να αποτρέπεται το πλεονέκτημα που θα είχαν οι πρώτοι που υιοθέτησαν το Proof of Burn πρωτόκολλο, υπάρχουν ενσωματωμένοι μηχανισμοί που προωθούν την περιοδική καύση των κρυπτονομισμάτων για την διατήρηση των εξορύξεων. Η ισχύς των καμένων κρυπτονομισμάτων, “αποσυντίθεται” ή μειώνεται κάθε φορά που ένα νέο μπλοκ εξορύσεται, πράγμα που το οποίο προωθεί την τακτική δραστηριότητα των εξορυκτών αντί να είναι μιας φοράς επένδυση. Για να διατηρήσουν ανταγωνιστικό πνεύμα, οι εξορύκτες μπορεί να επενδύουν περιοδικά σε καλύτερο εξοπλισμό καθώς εξελίσσεται η τεχνολογία.

Η υλοποίηση του Proof of Burn(PoB), μπορεί να προσαρμοστεί. Για παράδειγμα, το Slimcoin, ένα δίκτυο εικονικών κρυπτονομισμάτων που χρησιμοποιεί το Proof of Burn(PoB),

επιτρέπει στον εξορύκτη να “καίει” τα κρυπτονομίσματα που έπειτα του δίνουν το δικαίωμα να ανταγωνιστεί και για το επόμενο μπλοκ αλλά του δίνει και την ευκαιρία λάβει μπλοκ για μεγαλύτερο χρονικό διάστημα, για τουλάχιστον ένα έτος.

Ουσιαστικά, η υλοποίηση του Proof of Burn(PoB) στο Slimcoin, συνδυάζει τρεις αλγόριθμους, τους PoW, PoS και την βασική ιδέα του PoB. Η διαδικασία “καύσης” των νομισμάτων, χρησιμοποιεί τον αλγόριθμο PoW, όσο πιο πολλά νομίσματα θα “καούν”, τόσο περισσότερο θα μπορεί ο εξορύκτης να εξορύξει, εξασφαλίζοντας έτσι και τον αλγόριθμο POS, και όλη αυτή η διαδικασία ονομάζεται Proof of Burn(PoB).

Όσο πιο πολλά νομίσματα “κάψει” ο εξορύκτης, τόσο μεγαλύτερη εικονική δύναμη εξόρυξης έχει. Επομένως, όσο περισσότερα νομίσματα “καούν”, τόσο μεγαλύτερη ισχύ θα έχει, και το αντίστροφο. Στο πρωτόκολλο Proof of Work(PoW), με την υψηλότερη ισχύ εξόρυξης βελτιώνεται η ταχύτητα με την οποία βρίσκονται καινούργια μπλοκ και έχει ως συνέπεια ο εξορύκτης να κερδίζει περισσότερες ανταμοιβές.

Στα δίκτυα Proof of Burn(PoB), η διαδικασία “καύσης” των νομισμάτων περιλαμβάνει, να αποστέλλονται τα νομίσματα σε “eater” διευθύνσεις. Αυτές οι διευθύνσεις είναι δημόσια γνωστές αλλά δεν είναι προσβάσιμες καθώς παράγονται τυχαία και δεν έχουν κάποιο ιδιωτικό κλειδί.

Το Proof of Burn(PoB), είναι παρόμοιο με τον αλγόριθμο Proof of Stake(PoS), με την έννοια ότι και οι δύο μηχανισμοί, περιλαμβάνουν τα νομίσματά τους για να διασφαλίσουν την ασφάλεια του δικτύου τους. Παρόλα αυτά, σε αντίθεση με το Proof of Burn(PoB), τα νομίσματα που είναι κλειδωμένα σε συστήματα Proof of Stake(PoS) δεν διαγράφονται οριστικά και οι κάτοχοί τους έχουν πρόσβαση σε αυτά και μπορούν να τα πωλήσουν σε περίπτωση που θέλουν να αποχωρήσουν από το δίκτυο. Από την άλλη, τα νομίσματα που χρησιμοποιούν τον αλγόριθμο Proof of Burn(PoB), οδηγούν στην σπανιότητα του νομίσματος.

Ο αλγόριθμος Proof of Burn(PoB) είναι ένας νέος τύπος αλγορίθμου. Ως εκ τούτου, δεν έχει αποδειχθεί ακόμα ότι λειτουργεί σε μεγάλα δίκτυα. Μερικά προτερήματα του αλγόριθμου Proof of Burn(PoB), είναι ότι είναι βιώσιμος και η διαδικασία εξόρυξής του είναι αρκετά αποκεντρωμένη.

Αντίθετα με τις αποκεντρωμένες πλατφόρμες που βασίζονται στο PoW, όπως το bitcoin και το Ethereum, το PoB χρησιμοποιεί εικονικές εξέδρες για την επικύρωση των συναλλαγών. Με απλά λόγια, οι εξορύκτες PoB, ξεκινούν την καύση νομισμάτων για να δείξουν την συμμετοχή τους στο δίκτυο και να τους επιτραπεί να εξορύξουν. [18]

3.2. HARD FORKS/SOFT FORKS

Το hard fork (ή hardfork), είναι μια ριζική αλλαγή στο πρωτόκολλο ενός δικτύου που καθιστά τα μπλοκ και τις συναλλαγές του έγκυρες που δεν ήταν έγκυρες στο παρελθόν ή το αντίστροφο. Ένα hard fork απαιτεί από όλους τους κόμβους ή τους χρήστες να αναβαθμίσουν στην πιο πρόσφατη έκδοση του λογισμικού του πρωτοκόλλου.

Τα Forks μπορούν να ξεκινήσουν από προγραμματιστές ή από μια κοινότητα κρυπτογράφησης που δεν ικανοποιούνται με τις λειτουργίες που προσφέρονται από υπάρχουσες εφαρμογές του blockchain. Μπορεί επίσης να προκύψουν ως ένας τρόπος πληθοπορισμού χρηματοδότησης για έργα νέων τεχνολογιών ή προσφορές κρυπτονομισμάτων.

Τα hard forks και τα soft forks είναι ουσιαστικά τα ίδια, δηλαδή, όταν σε μια πλατφόρμα κρυπτονομισμάτων αλλάζει ο υπάρχων κώδικας της, μια παλιά έκδοση παραμένει στο δίκτυο ενώ δημιουργείται η νέα έκδοση. Όμως τα hard forks μπορούν να έρθουν σε αντίθεση με τα soft forks.

Ένα hard fork είναι όταν οι κόμβοι της πιο πρόσφατης έκδοσης ενός blockchain, δεν δέχονται τις παλαιότερες εκδόσεις της αλυσίδας μπλοκ και έτσι δημιουργείται μια μόνιμη απόκλιση από την προηγούμενη έκδοση του blockchain. Η προσθήκη ενός νέου κανόνα στον κώδικα δημιουργεί μια διχάλα στο blockchain: η μία διαδρομή ακολουθεί τη νέα, αναβαθμισμένη αλυσίδα μπλοκ και η άλλη διαδρομή συνεχίζει κατά μήκος της παλιάς διαδρομής. Γενικά, μετά από σύντομο χρονικό διάστημα, όσοι βρίσκονται στην παλιά αλυσίδα θα συνειδητοποιήσουν ότι η έκδοση του blockchain τους είναι ξεπερασμένη ή άσχετη και θα αναβαθμίσουν γρήγορα στην πιο πρόσφατη έκδοση.

Όλοι οι miners πρέπει να συμφωνήσουν για τους νέους κανόνες και για το τι περιλαμβάνει ένα έγκυρο μπλοκ στην αλυσίδα. Έτσι, όταν αλλαχτούν οι κανόνες, πρέπει να διαχωριστεί σε δύο - όπως μια διακλάδωση σε έναν δρόμο - για να αναδειχθεί ότι υπήρξε μια αλλαγή ή μια εκτροπή στο πρωτόκολλο. Οι προγραμματιστές μπορούν στη συνέχεια να ενημερώσουν όλο το λογισμικό ώστε να αντικατοπτρίζει τους νέους κανόνες.

Υπάρχουν διάφοροι λόγοι για τους οποίους οι προγραμματιστές θέλουν να εφαρμόσουν ένα hard fork, όπως η διόρθωση σημαντικών κινδύνων ασφαλείας που εντοπίζονται σε παλαιότερες εκδόσεις του λογισμικού ή για να προστεθεί μια νέα λειτουργικότητα ή για την αντιστροφή συναλλαγών.

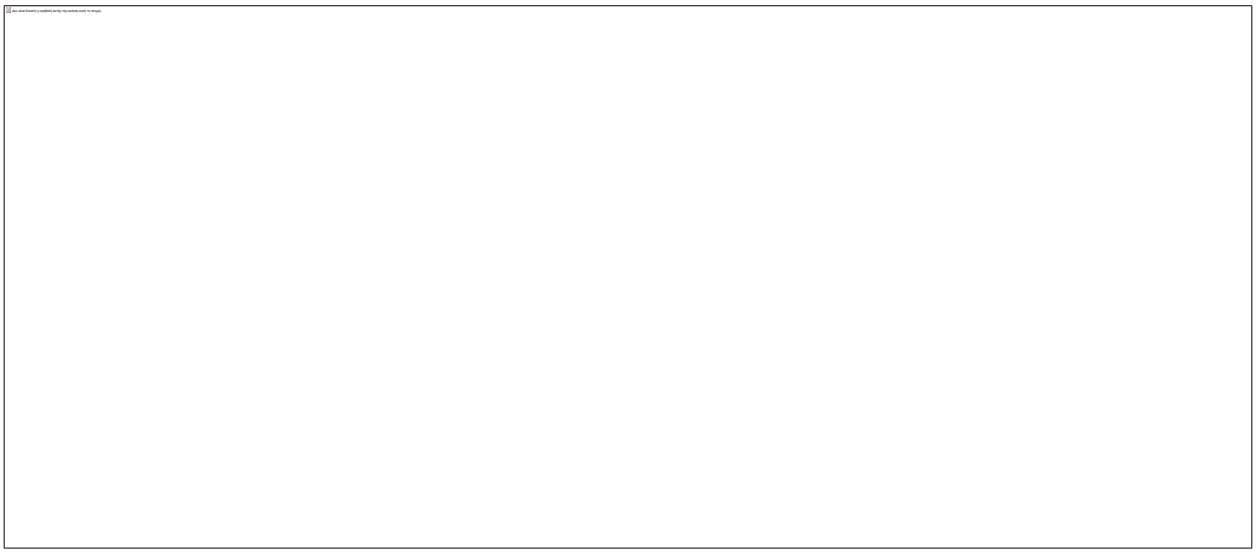
Μετά από ένα χακάρισμα στο δίκτυο του Ethereum, η κοινότητα του Ethereum ψήφισε σχεδόν ομόφωνα υπέρ ενός hard fork για την αναστολή των συναλλαγών που διέλυσαν το ψηφιακό νόμισμα αξίας δεκάδων εκατομμυρίων δολαρίων από έναν ανώνυμο χάκερ. Το hard forking βοήθησε επίσης τους κατόχους των DAO tokens να επιστραφούν τα κεφάλαιά τους που είχαν σε Ether (ETH).

Η πρόταση για ένα hard fork δεν ξετύλιξε ακριβώς το ιστορικό συναλλαγών του δικτύου. Αντίθετα, μετέφερε τα κεφάλαια που συνδέονται με το DAO σε ένα νέο smart contract με μοναδικό σκοπό να αφήσει τους αρχικούς ιδιοκτήτες να αποσύρουν τα κεφάλαιά τους.

Ένα fork σε μια αλυσίδα μπλοκ μπορεί να συμβεί σε οποιαδήποτε πλατφόρμα της κρυπτοτεχνολογίας - όχι μόνο στο Bitcoin ή στο Ethereum. Αυτό συμβαίνει επειδή τα blockchain και τα κρυπτονομίσματα λειτουργούν βασικά με τον ίδιο τρόπο, ανεξάρτητα από την πλατφόρμα στην οποία βρίσκονται. Μπορεί να σκεφτεί κανείς τα μπλοκ στο blockchain ως κρυπτογραφικά κλειδιά που μετακινούν μνήμη. Επειδή οι miners σε ένα blockchain θέτουν τους κανόνες που μετακινείται η μνήμη στο δίκτυο, αυτοί οι miners κατανοούν και τους νέους κανόνες.

Με ένα soft fork, μόνο ένα blockchain θα παραμείνει έγκυρο καθώς οι χρήστες ενημερώνονται. Ενώ με ένα hard fork, τόσο το παλιό όσο και το νέο blockchain συνυπάρχουν, πράγμα που σημαίνει ότι το λογισμικό πρέπει να ενημερωθεί για να λειτουργεί σύμφωνα με τους νέους κανόνες. Και τα δύο forks δημιουργούν ένα διαχωρισμό, αλλά ένα hard fork δημιουργεί δύο μπλοκ αλυσίδων και ένα sort fork θα οδηγήσει σε ένα.

Λαμβάνοντας υπόψη τις διαφορές στην ασφάλεια μεταξύ hard fork και ενός soft fork, σχεδόν όλοι οι χρήστες και οι προγραμματιστές ζητούν ένα hard fork, ακόμη και όταν ένα soft fork φαίνεται ότι μπορεί να κάνει τη δουλειά του. Η προσεκτική εξέταση και η διόρθωση των μπλοκ σε ένα blockchain απαιτεί τεράστια υπολογιστική ισχύ, αλλά το απόρρητο που αποκτάται από ένα hard fork είναι πιο λογικό από τη χρήση ενός soft fork. [12]



Εικόνα 9: Παράδειγμα διαγράμματος των Fork από την σελίδα Investopedia[12]

3.3. Κινητά πορτοφόλια

Το κινητό πορτοφόλι είναι ένα εικονικό πορτοφόλι που έχει αποθηκευμένους τρόπους πληρωμής σε μια κινητή συσκευή. Είναι ένας βολικός τρόπος του χρήστη για να πραγματοποιεί αγορές σε καταστήματα και μπορεί να χρησιμοποιηθεί και σε εμπόρους που έχουν καταχωρηθεί σαν πάροχοι υπηρεσιών κινητών πορτοφολιών.

Η σχέση επιχείρηση-καταναλωτή αλλάζει γρήγορα σε ψηφιακή. Από τις πλατφόρμες ηλεκτρονικού εμπορίου μέχρι και τους σύμβουλους ρομπότ, οι επιχειρήσεις αλλάζουν τον τρόπο λειτουργίας τους για να ανταποκρίνονται στις διαρκώς μεταβαλλόμενες ανάγκες των πελατών τους και την αυξανόμενη χρήση κινητών τηλεφώνων και άλλων συσκευών. Εμφανίζονται εταιρείες στον χρηματοοικονομικό τομέα οι οποίες προσφέρουν ψηφιακές πλατφόρμες/λύσεις και αναγνωρίζονται ως μέρη του κλάδου της οικονομικής τεχνολογίας.

Αυτές οι αναδυόμενες εταιρείες, δημιουργούν διάσπαρτα εργαλεία και υπηρεσίες που είναι εύκολα προσβάσιμες σε χαμηλές τιμές. Ένας από τους τομείς του χρηματοπιστωτικού κλάδου που είναι γεμάτος καινοτομίες, είναι ο τομέας των πληρωμών. Χρησιμοποιώντας την κινητή τεχνολογία όπως για παράδειγμα τα κινητά τηλέφωνα, τα tablet και τα smartwatches, οι εταιρείες και οι χρήστες, προσαρμόζονται σε διαδικτυακές και μη συναλλαγές με την χρήση ενός κινητού πορτοφολιού.

Το κινητό πορτοφόλι μπορεί πολύ εύκολα να εγκατασταθεί σε ένα κινητό τηλέφωνο ή να είναι μια υπάρχουσα εφαρμογή μέσα στο κινητό τηλέφωνο. Ένα κινητό πορτοφόλι αποθηκεύει τις πληροφορίες της πιστωτικής κάρτας, της χρεωστικής κάρτας, των κουπονιών ή άλλων καρτών πληρωμής. Μόλις εγκατασταθεί η εφαρμογή και ο χρήστης εισάγει τις πληροφορίες πληρωμής του, το πορτοφόλι αποθηκεύει αυτές τις πληροφορίες, συνδέοντας το με μια προσωπική μορφή αναγνώρισης όπως για παράδειγμα έναν αριθμό ή ένα κλειδί, έναν κωδικό QR ή μια εικόνα του σε κάθε κάρτα που είναι αποθηκευμένη.

Δεν είναι όλα τα smartphones και οι φορητές συσκευές εξοπλισμένες με τεχνολογία nfc, συμπεριλαμβανομένων και των iPhone. Για τους χρήστες iPhone, υπάρχουν διαφορετικοί τρόποι για να χρησιμοποιήσουν τα κινητά πορτοφόλια τους και να πραγματοποιήσουν πληρωμές σε κάποιο κατάστημα. Του PayPal το κινητό πορτοφόλι επιτρέπει στους χρήστες του, να πραγματοποιήσουν πληρωμές χρησιμοποιώντας το κινητό τους τηλέφωνο κατά την ολοκλήρωση της αγοράς.

Το κινητό τηλέφωνο πρέπει να συνδέεται με του χρήστη τον λογαριασμό PayPal για να εγκριθεί η συναλλαγή. Ενώ η PayPal χρησιμοποιεί τα κινητά τηλέφωνα, άλλες εταιρείες χρησιμοποιούν διαφορετικές μεθόδους αναγνώρισης των προσωπικών στοιχείων του χρήστη. Το LevelUp είναι ένα κινητό πορτοφόλι που χρησιμοποιεί κωδικούς QR τα οποία σκανάρονται μόλις τελειώσει ο χρήστης τις αγορές του. Το Square Wallet, χρησιμοποιούσε την εικόνα του χρήστη, η οποία επαληθεύονταν εύκολα από κάποιον ταμεία.

Οι κακοπροαίρετες δραστηριότητες, όπως η κλοπή ταυτότητας, γίνονται πιο δύσκολες όταν στοχεύουν τα κινητά πορτοφόλια. Ενώ η πιστωτική κάρτα ενός ατόμου μπορεί εύκολα να κλαπεί ή να αντιγραφεί, τα κινητά τηλέφωνα δεν μπορούν να κλαπούν το ίδιο εύκολα. Ένα κλεμμένο κινητό τηλέφωνο που χρησιμοποιεί κάποιον κωδικό πρόσβασης ή δαχτυλικό αποτύπωμα, δεν έχει τόσο εύκολη πρόσβαση.

Τα κινητά πορτοφόλια μπορεί επίσης να έχουν κρυπτογραφημένα κλειδιά, καθώς και να είναι χρήσιμα για επιχειρήσεις λιανικής που αντιμετωπίζουν μεγάλους όγκους συναλλαγών καθημερινά, διότι τα κινητά πορτοφόλια μπορούν να μειώσουν τους χρόνους αναμονής και πληρωμής. Αυτό συμφέρει και την επιχείρηση και τον καταναλωτή.

Επειδή τα κινητά πορτοφόλια είναι μια ψηφιακή έκδοση των κανονικών πορτοφολιών, σχεδόν κάθε χρήσιμη κάρτα που έχει ένα αληθινό πορτοφόλι, μπορεί να μεταφερθεί και στο κινητό πορτοφόλι όπως το δίπλωμα οδήγησης, ο αριθμός κοινωνικής ασφάλισης, οι κάρτες υγείας καθώς και εισιτήρια λεωφορείων και τρένων.

Τα ψηφιακά πορτοφόλια συχνά χρησιμοποιούνται εναλλακτικά με τα κινητά πορτοφόλια. Ενώ ωστόσο και τα δύο έχουν πληροφορίες πληρωμής, εφαρμόζονται διαφορετικά. Τα ψηφιακά πορτοφόλια συνήθως χρησιμοποιούνται για online αγορές και δεν είναι απαραίτητο να χρησιμοποιηθούν σε κινητές συσκευές. Τα κινητά πορτοφόλια χρησιμοποιούνται συνήθως από άτομα που δεν θέλουν να κουβαλάνε πάνω τους το πορτοφόλι τους όταν κάνουν αγορές από καταστήματα, για αυτόν τον λόγο, τα κινητά πορτοφόλια πρέπει να βρίσκονται μέσα σε κινητές συσκευές, όπως είναι το Google Pay, το Samsung Pay και το Apple Pay που μπορούν να εγκατασταθούν σε ένα κινητό ή ένα smartwatch. Ένας κανονικός λογαριασμός PayPal, είναι μια μορφή ψηφιακού πορτοφολιού, αλλά όταν χρησιμοποιείται σε συνδυασμό με υπηρεσίες πληρωμών μέσω κινητού τηλεφώνου και κινητές συσκευές, λειτουργεί σαν ένα κινητό πορτοφόλι. [19,20,21]

3.3.1. Ψηφιακό πορτοφόλι

Το ψηφιακό πορτοφόλι είναι ένα σύστημα λογισμικού που αποθηκεύει με ασφάλεια τις πληροφορίες του χρήστη και τους κωδικούς του για διάφορες μεθόδους πληρωμής και ιστοσελίδων. Χρησιμοποιώντας ένα ψηφιακό πορτοφόλι, οι χρήστες μπορούν να ολοκληρώσουν εύκολα και γρήγορα τις πληρωμές τους χρησιμοποιώντας τεχνολογία nfc. Μπορούν επίσης να χρησιμοποιούν δυσκολότερους κωδικούς, χωρίς να χρειάζεται να τους θυμούνται αργότερα.

Τα ψηφιακά πορτοφόλια μπορούν να χρησιμοποιηθούν σε συνδυασμό με συστήματα πληρωμών μέσω κινητών τηλεφώνων, και τους επιτρέπουν να κάνουν πληρωμές με το κινητό τους τηλέφωνο. Ένα ψηφιακό πορτοφόλι μπορεί να χρησιμοποιηθεί για την αποθήκευση και άλλων πληροφοριών, όπως κουπονιών. Τα ψηφιακά πορτοφόλια, είναι οικονομικοί λογαριασμοί που επιτρέπουν στους χρήστες, να αποθηκεύσουν ποσά κεφαλαίων, να κάνουν συναλλαγές και να παρακολουθούν τα ιστορικά των συναλλαγών τους μέσα από έναν υπολογιστή.

Αυτό το λογισμικό, μπορεί να περιλαμβάνεται σε εφαρμογές για κινητά μιας τράπεζας, ή ως πλατφόρμα πληρωμών όπως το Alipay και το PayPal. Τα ψηφιακά πορτοφόλια είναι επίσης ο τρόπος αγορών κρυπτονομισμάτων όπως το bitcoin.

Τα ψηφιακά πορτοφόλια εξαλείφουν κατά πολύ την ανάγκη να έχει ο χρήστης πάνω του ένα πορτοφόλι καθώς αποθηκεύουν όλες τις πληροφορίες του χρήστη σε ένα ασφαλές περιβάλλον, όπως επίσης τα ψηφιακά πορτοφόλια μπορούν να τα εκμεταλλευτούν εταιρείες που συλλέγουν πληροφορίες καταναλωτών. Όσο πιο πολύ γνωρίζουν οι εταιρείες για τις καταναλωτικές συνήθειες των πελατών τους, τόσο πιο στοχευμένα μπορούν να διαφημίζουν τα προϊόντα τους. Το μειονέκτημα για τους καταναλωτές μπορεί να είναι η απώλεια της ιδιωτικής τους ζωής.

Τα ψηφιακά πορτοφόλια επιτρέπουν σε πολλές αναπτυσσόμενες χώρες να εντάσσονται πληρέστερα στο παγκόσμιο χρηματοοικονομικό σύστημα, όπως επίσης επιτρέπουν στους συμμετέχοντες να δέχονται πληρωμές για τις υπηρεσίες τους, καθώς και να λαμβάνουν κεφάλαια από συγγενείς και φίλους. Τα ψηφιακά πορτοφόλια δεν απαιτούν κάποιον τραπεζικό λογαριασμό και συνήθως επιτρέπουν τα άτομα να ανοίξουν έναν λογαριασμό χωρίς τραπεζικό λογαριασμό ή κοινότητες όπως την Blank και την Latinx καθώς επίσης και στις αγροτικές περιοχές με χαμηλό εισόδημα τους επιτρέπει να εξυπηρετηθούν και έτσι επιτρέπει μια ευρύτερη οικονομική τάξη.

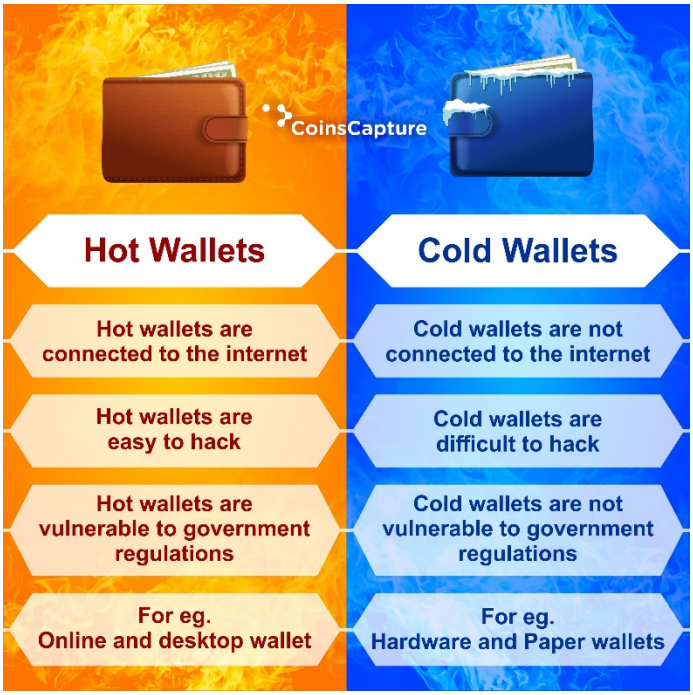
Τα κρυπτονομίσματα βασίζονται αποκλειστικά σε ψηφιακά πορτοφόλια για την διατήρηση των υπολοίπων τους και για να πραγματοποιούν συναλλαγές. Ενώ υπήρχαν μια πληθώρα ψηφιακών πορτοφολιών το 2020, τα τρία μεγαλύτερα είναι της Google, της Amazon και της Apple. Για παράδειγμα, η υπηρεσία της Google, επιτρέπει στους χρήστες της να αποθηκεύουν χρήματα στον λογαριασμό τους. Οι χρήστες, μπορούν να ξοδέψουν αυτά τα χρήματα σε φυσικά και online καταστήματα καθώς και σε επιχειρήσεις που αποδέχονται το ψηφιακό πορτοφόλι της Google.

Όπως σημειώθηκε παραπάνω, αυτό γίνεται εφικτό με την τεχνολογία nfc(η επικοινωνία δύο συσκευών να επικοινωνούν αν βρίσκονται σε κοντινή απόσταση). Αν μια επιχείρηση δεν αποδέχεται πληρωμές μέσω της Google, η Google ανέπτυξε πρόσφατα και μια φυσική κάρτα(μια χρεωστική κάρτα) που είναι συνδεδεμένη με την τράπεζα της Google. Πρόσφατα η Google συνδύασε τις 2 βασικές της ροές πληρωμών, το Android Pay και το Google Wallet σε μια υπηρεσία που αποκαλείται Google Pay. Η Apple από την άλλη μεριά, συνεργάστηκε με την εταιρεία Goldman Sachs του Warren Buffet για να δημιουργήσει πιστωτικές κάρτες της Apple και να επεκτείνει τις υπηρεσίες της ApplePay.

Τα ψηφιακά πορτοφόλια από την πλευρά του διακοσμητή, γίνονται δημοφιλείς ανάμεσα στους μεγάλους εμπόρους λιανικής λόγο της ασφάλειας, της χρησιμότητας και της αποτελεσματικότητας που παρέχει στον τελικό χρήστη πράγμα που αυξάνει την ικανοποίησή τους από την τελική τους αγορά.

Υπάρχουν δύο ειδών ψηφιακών πορτοφολιών, τα κρύα πορτοφόλια και τα ζεστά. Τα ζεστά πορτοφόλια έχουν μια συνεχείς σύνδεση στο διαδίκτυο ενώ τα κρύα πορτοφόλια δεν συνδέονται διαδικτυακά. Τα ζεστά πορτοφόλια χρησιμοποιούνται κυρίως για την αγορά και ανταλλαγή αγαθών, ενώ τα κρύα πορτοφόλια έχουν μέσα τους έναν αποθηκευμένο αριθμό χρημάτων.

Ενώ παρέχουν επιλύσεις για διαφορετικές ανάγκες, οι δύο τύποι ψηφιακών πορτοφολιών έχουν και διαφορά στην ασφάλεια. Ένα ζεστό πορτοφόλι επειδή είναι συνδεδεμένο διαδικτυακά, είναι πιο ευαίσθητο και ευάλοτο σε επιθέσεις από χάκερ. Από την άλλη, τα κρύα πορτοφόλια είναι πολύ πιο ασφαλές σε επιθέσεις καθώς δεν είναι συνδεδεμένα στο διαδίκτυο. [19,20,21]



Εικόνα 10: Διαφορές μεταξύ hot(αριστερά) και cold(δεξιά) wallet[40]

3.4. DeFi

Το DeFi είναι συντομογραφία της «Decentralized Finance», ένας γενικός όρος για μια ποικιλία οικονομικών εφαρμογών σε κρυπτονομίσματα ή blockchain που στοχεύουν στη διακοπή των χρηματοπιστωτικών διαμεσολαβητών. Σε έναν χρηματοοικονομικό κόσμο που γίνεται όλο και πιο ψηφιακός, το DeFi εστιάζει στο να προσφέρει στους επενδυτές την ευκολία των συναλλαγών peer-to-peer. Αξιοποιώντας την αποτελεσματικότητα και τη δύναμη των έξυπνων συμβολαίων —ψηφιακά συμβόλαια που ισχύουν στο blockchain—. Οι πλατφόρμες DeFi δημιουργούν έναν χώρο δανεισμού, συναλλαγών, αποταμίευσης και απόκτησης τόκων που δεν απαιτεί όλη τη συνήθη γραφειοκρατία και τις μικρολεπτομέρειες.

Το DeFi εμπνέεται από το blockchain, την τεχνολογία πίσω από το ψηφιακό νόμισμα bitcoin, το οποίο επιτρέπει σε πολλές οντότητες να διατηρούν ένα αντίγραφο ενός ιστορικού

συναλλαγών, πράγμα που σημαίνει ότι δεν ελέγχεται από μια ενιαία, κεντρική πηγή. Αυτό είναι σημαντικό επειδή τα κεντρικά συστήματα και οι ανθρώπινοι φύλακες μπορούν να περιορίσουν την ταχύτητα και την πολυπλοκότητα των συναλλαγών, ενώ προσφέρουν στους χρήστες λιγότερο άμεσο έλεγχο των χρημάτων τους. Το DeFi είναι ξεχωριστό επειδή επεκτείνει τη χρήση του blockchain από απλή ανταλλαγή ή/και μεταφορά αξιών σε πιο περίπλοκες περιπτώσεις οικονομικής χρήσης.

Οι στόχοι του DeFi είναι οι εξής:

- Η αφαίρεση όλης της γραφειοκρατίας, τα έξυπνα συμβόλαια(smart contracts) επεξεργάζονται την τεχνολογία του blockchain, επομένως δεν υπάρχουν χαρτιά, ούτε χρόνος αναμονής όπως στην τράπεζας για την εκκαθάριση των συναλλαγών.

- Η αφαίρεση του τρίτου, μη χρήσιμου ατόμου, δηλαδή η αυτοματοποίηση της διαδικασίας συμβολαίων στο blockchain εξαλείφει την ανάγκη για ανθρώπινους μεσάζοντες, μη καθιστώντας αναγκαία την συμμετοχή εξωτερικών διαμεσολαβητών, όπως οι δικηγόροι, για την επεξεργασία συμφωνιών μεταξύ των μερών.

- Το DeFi κάνει την επιχειρηματική δραστηριότητα πιο απρόσκοπτη και γρήγορη εμπειρία από την αρχή μέχρι το τέλος εφόσον δεν θα υπάρχουν εξαρτήσεις από διάφορα μέλη ή χρόνους αναμονής.

- Πολλές από τις οικονομικές ευκαιρίες που προσφέρονται μέσω των DeFi platforms προορίζονται συνήθως για μεγάλα χρηματοπιστωτικά ιδρύματα όπως τα hedge funds και οι τράπεζες. Το DeFi προσπαθεί να κλείσει το χάσμα μεταξύ του ατόμου και της οικονομικής ολιγαρχίας.

Τα 10 μεγαλύτερα αυτή την στιγμή DeFi projects είναι από τα παρακάτω tokens:

Το Aave (AAVE), ξεκίνησε το 2017 με το όνομα ETHLend και είναι μια από τις αρχικές πλατφόρμες DeFi στην αγορά. Η Aave είναι μια αποκεντρωμένη πλατφόρμα ρευστότητας που επιτρέπει τον δανεισμό περιουσιακών στοιχείων και την απόκτηση ανταμοιβών στις καταθέσεις. Συγκεντρώνει δανειστές και δανειολήπτες σε έναν αποκεντρωμένο χώρο για να επιτρέψει ένα σύστημα δανεισμού ίσων ευκαιριών. Επίσης μπορεί κανείς να κερδίσει ανταμοιβές και εκπτώσεις κάνοντας staking με το AAVE στην πλατφόρμα Aave DeFi.

Η Avalanche (AVAX) εμπορεύεται τον εαυτό της ως «the fastest smart contract platform in the blockchain Industry», ενώ επίσης εδραιώνει τη θέση της στον αναπτυσσόμενο χώρο non fundable tokens(NFT) και χτίζει συνδεσιμότητα με άλλα έργα blockchain όπως το SushiSwap (SUSHI), το Chainlink (LINK) και το Graph (GRT). Το έργο του τοποθετείται ως άμεσος αντίπαλος του Ethereum λόγω της ικανότητάς του να παρέχει φθηνότερες συναλλαγές σε κλάσματα του χρόνου. Η Avalanche ολοκλήρωσε πρόσφατα χρηματοδότηση 230 εκατομμυρίων δολαρίων για

να υποστηρίξει τις πρωτοβουλίες της στο DeFi, καθιστώντας την ένα συναρπαστικό μέρος για τη δημιουργία καταστημάτων για έργα DeFi.

Το Cardano (ADA), ένα από τα μεγαλύτερα έργα blockchain στον κόσμο, αποκαλείται μερικές φορές το «Green Blockchain» λόγω των εντυπωσιακών αναφορών χρήσης ενέργειας και του πρωτοκόλλου του στην απόδειξης συμμετοχής(proof of stake). Το Cardano ανακοίνωσε τον Σεπτέμβριο του 2021 ότι λαμβάνει μια ώθηση στο οικοσύστημα από την πρόσφατη επένδυσή 100 εκατομμυρίων δολαρίων στην αποκεντρωμένη χρηματοδότηση, τα NFTs και την εκπαίδευση στο blockchain.

Η Chainlink (LINK) είναι μια αποκεντρωμένη υπηρεσία oracle που στοχεύει στη σύνδεση έξυπνων συμβάσεων με δεδομένα από τον πραγματικό κόσμο χρησιμοποιώντας την τεχνολογία της Oracle. Η Chainlink ανακοίνωσε πρόσφατα την έναρξη μιας Προγραμματιζόμενης Γέφυρας Token που θα επιτρέψει νέα επικοινωνία μεταξύ των blockchains του DeFi. Αυτό θα βοηθήσει το DeFi να κλιμακωθεί σωστά και να αποφύγει τα σημεία συμφόρησης που εμποδίζουν τις προηγούμενες γενιές έργων blockchain.

Το Polkadot (DOT) διευκολύνει το διαδίκτυο όπου ανεξάρτητες αλυσίδες μπλοκ μπορούν να ανταλλάσσουν πληροφορίες και συναλλαγές με τρόπο αξιόπιστο μέσω της αλυσίδας αναμετάδοσης Polkadot. Αυτό καθιστά το Polkadot και τα έργα που επιλέγουν να βασίζονται στο Polkadot, πολύ πιο γρήγορα και επεκτάσιμα από την τρέχουσα προσφορά του Ethereum. Λειτουργώντας ως θεμέλιο για να αξιοποιηθούν τα έργα DeFi, βοηθά την ανάπτυξη και τις δυνατότητες του δικτύου στο σύνολό του.

Η Terra Luna (LUNA) είναι μια πλατφόρμα έξυπνων συμβολαίων επόμενης γενιάς που συνδυάζει την αποκεντρωμένη χρηματοδότηση(DeFi) με την έννοια των stablecoins. Η πλατφόρμα του υποστηρίζει stablecoins που προσφέρουν άμεσους διακανονισμούς, χαμηλές χρεώσεις και απρόσκοπτη διασυνοριακή ανταλλαγή. Το Luna λειτουργεί ως η ασταθής ραχοκοκαλιά που κρατά την Terra, την αδερφή της στα stablecoin, ισορροπημένη και γειωμένη. Η προσθήκη της αναδυόμενης δημοτικότητας του DeFi στη σοβαρή προσοχή που προσελκύουν τα stablecoins —από τους καταναλωτές όσο και από τις κυβερνήσεις— κάνει το LUNA να παρακολουθεί.

Το Polygon (MATIC) είναι ένα από τα πιο καλά υιοθετημένα και ταχύτερα Layer 2 του Ethereum πάνω στις λύσεις κλιμάκωσης και στα αποκεντρωμένα οικοσυστήματα εφαρμογών. Διαθέτει χαρακτηριστικά όπως διαλειτουργικότητα, επεκτασιμότητα και ασφάλεια. Ουσιαστικά, το Polygon προσθέτει «μερικές λωρίδες κυκλοφορίας στον πολυταξιδεμένο αυτοκινητόδρομο» Ethereum Layer 1. Η πλειοψηφία των έργων στο DeFi στεγάζεται επί του παρόντος στο blockchain του Ethereum. Επομένως, λιγότερη συμφόρηση στο Ethereum σημαίνει μεγαλύτερες ταχύτητες και περισσότερα οφέλη για το οικοσύστημα DeFi.

Το Solana (SOL) φέρνει επανάσταση στους μηχανισμούς συναίνεσης με την δημιουργία της απόδειξης της ιστορίας(proof of history). Αυτό σημαίνει ότι, αντί για mining ή staking στην

πλατφόρμα για την επικύρωση συναλλαγών, όλες οι συναλλαγές αποδεικνύονται αληθινές με μια χρονική σήμανση στο blockchain. Το Solana είναι γνωστό ως ο κύριος ανταγωνιστής του Ethereum επειδή παρέχει γρήγορες ταχύτητες ενώ εξακολουθεί να είναι στην πλατφόρμα Layer 1, πράγμα που σημαίνει ότι δεν χρειάζεται βοήθεια από άλλη πλατφόρμα για να εκτελέσει αυτές τις γρήγορες συναλλαγές.

Το Synthetix (SNX, ένα ταχέως αναπτυσσόμενο αποκεντρωμένο χρηματιστήριο) επιτρέπει τα κρυπτονομίσματα να μπορούν να ανταλλαχθούν για μετοχές, νομίσματα, εμπορεύματα και άλλα περιουσιακά στοιχεία που εξακολουθούν να κυριαρχούνται από τα παραδοσιακά χρηματιστήρια της Wall Street, του Λονδίνου και του Χονγκ Κονγκ. Το πιο μοναδικό χαρακτηριστικό του είναι ότι επιτρέπει στους χρήστες να δημιουργούν τα δικά τους συνθετικά περιουσιακά στοιχεία, που ονομάζονται "synths", επιτρέποντας την μετατροπή τους σε fiat, commodities, κρυπτονομίσματα και διαφορετικές κατηγορίες περιουσιακών στοιχείων. Παραδείγματα περιλαμβάνουν Bitcoin, ευρώ, USD, μετοχές Tesla, χρυσό κ.λπ. Αυτό σημαίνει ότι οι χρήστες μπορούν να στοιχηματίσουν στην τιμή ενός περιουσιακού στοιχείου χωρίς να χρειάζεται να κρατήσουν το πραγματικό περιουσιακό στοιχείο, γεγονός που έχει μετατρέψει το Synthetix σε ένα από τα πιο διαθέσιμα προϊόντα στο DeFi.

Το Uniswap (UNI) είναι ένα αποκεντρωμένο χρηματιστήριο που επιτρέπει στους χρήστες του να αγοράζουν και να παρέχουν ρευστότητα απευθείας από τα πορτοφόλια κρυπτογράφησης τους με ελάχιστο κόστος. Το AMM του (automated market maker) παρέχει άφθονη ρευστότητα για ισχυρή κίνηση και γρήγορες συναλλαγές στην πλατφόρμα του. Λόγω της δημοτικότητάς του, το token της Uniswap, το UNI, μπορεί να βρεθεί σε επενδυτικές πλατφόρμες εκτός του δικτύου DeFi, όπως το Voyager.

Κλείνοντας, οι πλατφόρμες DeFi αυτήν την στιγμή αναδεικνύονται ως πολύ σημαντικές τόσο από τους καταναλωτές όσο και από τους επενδυτές. Τα κεφάλαια DeFi συγκεντρώνουν εκατομμύρια δολάρια κάθε μέρα για να προωθήσουν πρωτοβουλίες, να βελτιώσουν και να δημιουργήσουν πλατφόρμες και να αναπτύξουν το ήδη ακμάζον δίκτυο. Αυτές οι εξελίξεις ανοίγουν το δρόμο προς την οικονομική ισότητα αυξάνοντας την προσβασιμότητα σε σημαντικά και κατά τα άλλα ανέφικτα χρηματοοικονομικά εργαλεία. Το DeFi, εξαλείφει το κενό καθιστώντας τα εμπόδια που οδήγησαν στην οικονομική πρόοδο για τους λίγους πολύ πλούσιους, να ανήκουν στο παρελθόν. Το μέλλον του DeFi είναι ήδη εδώ και είναι για όλους.

Οι περισσότερες DeFi εφαρμογές έχουν φτιαχτεί πάνω στο οικοσύστημα του Ethereum, η οποία ξεχωρίζει από το Bitcoin λόγο της μεγαλύτερης ευκολίας στην χρήση της καθώς είναι και πιο εύκολη η δημιουργία άλλων αποκεντρωμένων εφαρμογών με βάση το Ethereum. Αυτές οι περιπτώσεις χρήσης επισημάνθηκαν και από τον Vitalik Buterin το 2013, τον δημιουργό του Ethereum μέσα στο white paper του δικτύου Ethereum.

Αυτό συμβαίνει λόγο των έξυπνων συμβολαίων τα οποία εκτελούν ένα κομμάτι κώδικα αυτόματα όταν υπάρξουν ορισμένες συνθήκες και έτσι είναι πολύ πιο ευέλικτα. Ορισμένες γλώσσες του Ethereum όπως είναι το Solidity έχουν σχεδιαστεί ειδικά για την συγγραφή

έξυπνων συμβολαίων. Χάρη στα έξυπνα συμβόλαια, δεκάδες εφαρμογές DeFi έχουν γραφτεί πάνω στο δίκτυο του Ethereum.

Τα μεγαλύτερα είδη των DeFi είναι τα εξής:

- Decentralized exchanges (Dexes): Τα Dexes βοηθούν τους χρήστες να ανταλλάσσουν κρυπτονομίσματα με άλλα συναλλάγματα, όπως με δολάρια, ευρώ, κ.ά. Τα Dexes λειτουργούν μέσω του διαδικτύου αποκλειστικά και δεν απαιτούν κάποιον μεσάζοντα για τις ανταλλαγές.
- Stablecoins: Τα stablecoins είναι κρυπτονομίσματα τα οποία συνδέονται με τον πραγματικό κόσμο και έτσι είναι ισότιμα πάντα με ένα δολάριο.
- Πλατφόρμες δανεισμού: Αυτές οι πλατφόρμες χρησιμοποιούν έξυπνα συμβόλαια για να αντικαταστήσουν τους μεσάζοντες όπως για παράδειγμα είναι οι τράπεζες.
- "Wrapped" Bitcoins(WBTC): Το WBTC είναι ένας τρόπος αποστολής bitcoin στο δίκτυο του Ethereum έτσι ώστε το bitcoin να χρησιμοποιηθεί από τις εφαρμογές των DeFis απευθείας. Το WBTC επιτρέπει στους χρήστες τους να λαμβάνουν ένα ποσό επιτοκίου επειδή δανείζουν τα bitcoins τους μέσω της αποκεντρωμένης πλατφόρμας δανεισμού που αναλύσαμε παραπάνω.
- Αγορές πρόβλεψης: Οι αγορές πρόβλεψης είναι αγορές που προωθούν τον στοιχηματισμό μελλοντικών γεγονότων όπως είναι οι εκλογές. Ο στόχος αυτών των αγορών είναι να πετύχουν το ίδιο καλά χωρίς να υπάρχουν οι μεσάζοντες.

Εκτός των παραπάνω, έρχονται στο προσκήνιο και μερικές καινούργιες χρησιμότητες των DeFis:

- Yield Farming: Οι έμπειροι έμποροι που είναι πρόθυμοι να ρισκάρουν, μπορούν να χρησιμοποιήσουν το Yield Farming, όπου ο χρήστης αναλύει διάφορα DeFi tokens ψάχνοντας ευκαιρίες για τις μεγαλύτερες αποδόσεις.
- Liquidity mining: Είναι όταν οι εφαρμογές DeFi προσελκύουν χρήστες δίνοντάς τους δωρεάν tokens από την πλατφόρμα. Αυτή είναι και μια από τις πιο έντονες μορφές Yield Farming.
- Σύνθεση: Οι DeFi εφαρμογές είναι ανοιχτού κώδικα που σημαίνει ότι είναι διαθέσιμες να τις διαβάσει οποιοσδήποτε θέλει. Ως εκ τούτου, αυτές οι εφαρμογές μπορούν να χρησιμοποιηθούν για να συνθέσουν νέες εφαρμογές με τον κώδικά τους ως δομικό στοιχείο.
- Money lego: Θέτοντας διαφορετικά την έννοια της σύνθεσης, οι εφαρμογές DeFi είναι σαν τα Lego, τα μπλοκ παιχνιδιών που χρησιμοποιούν τα παιδιά για να κατασκευάσουν κτήρια, οχήματα και ούτω καθεξής. Οι εφαρμογές DeFi μπορούν να συνενωθούν με παρόμοιο τρόπο για τη δημιουργία νέων χρηματοοικονομικών προϊόντων. [27]

3.4.1. Πλατφόρμες δανεισμού

Αυτές οι πλατφόρμες είναι γνωστές μορφές των DeFi, οι οποίες συνδέουν τους δανειολήπτες με τους δανειστές κρυπτονομισμάτων. Η Compount, μια δημοφιλής πλατφόρμα

δανεισμού, επιτρέπει στους χρήστες της να δανείζονται κρυπτονομίσματα ή να δανείζουν με κάποιο επιτόκιο. Οι χρήστες κερδίζουν χρήματα με τον δανεισμό των κρυπτονομισμάτων. Η Compount καθορίζει τους τόκους αλγοριθμικά, έτσι ώστε αν υπάρχει μεγάλη ζήτηση για τον δανεισμό ενός κρυπτονομίσματος, οι τόκοι θα αυξηθούν ανάλογα.

Ο δανεισμός μέσα από το DeFi βασίζεται σε εξασφαλίσεις που σημαίνει ότι για να λάβει κάποιος δάνειο, θα πρέπει να παρέχει κάποια ασφάλεια (συχνά η ασφάλεια είναι στην μορφή ether που είναι το token του δικτύου του Ethereum). Έτσι οι χρήστες δεν χρειάζεται να δώσουν τα προσωπικά τους στοιχεία για να λάβουν ένα δάνειο όπως λειτουργούν τα κανονικά δάνεια.[27]

3.4.2. Stablecoins

Μια άλλη μορφή των DeFi είναι τα Stablecoins. Τα κρυπτονομίσματα συχνά έχουν πιο απότομες εναλλαγές στις τιμές τους από ότι το απλό το χρήμα, το οποίο δεν είναι καλό για τους Day traders(έμποροι που μετατρέπουν το χρήμα τους σε μετοχές ή κρυπτονομίσματα τακτικά με σκοπό το γρήγορο κέρδος) το οποίο υποδεικνύει ότι το κρυπτονόμισμα δεν είναι υγειές και δεν μπορούν να προβλέψουν πόσο θα ανέβει το ποσό τους σε μια εβδομάδα. Τα Stablecoins συνδέουν τα tokens τους με την σταθερή τιμή του δολαρίου προκειμένου να διατηρηθεί η τιμή του υπό έλεγχο. Όπως υποδηλώνει και το όνομα, τα Stablecoins, στοχεύουν να φέρουν σταθερότητα στις τιμές τους.[27]

3.4.3. Αγορές πρόβλεψης

Μια από τις παλαιότερες εφαρμογές DeFi μέσα στο Ethereum είναι η λεγόμενη "πρόβλεψη αγοράς", όπου οι χρήστες στοιχηματίζουν στο αποτέλεσμα ενός μελλοντικού συμβάντος όπως είναι ποιος θα είναι ο επόμενος πρόεδρος της Αμερικής. Ο στόχος της συμμετοχής είναι προφανώς το κέρδος χρημάτων, ενώ μερικές φορές είναι πιο εύστοχες από άλλες μεθόδους όπως δημοσκοπήσεις.

Μερικές από τις κεντρικές αγορές πρόβλεψης είναι η Intrade και η PredictIt. Τα DeFi έχουν την δυνατότητα να ανεβάσει τους τόκους στις αγορές πρόβλεψης εφόσον παραδοσιακά αποδοκιμάζονται από τις κυβερνήσεις και συχνά κλείνουν όταν λειτουργούν με κεντρικό τρόπο. [8,27]

3.5. Stock market/Crypto market

Το crypto market, παρόμοια με το stock market είναι η πράξη της κερδοσκοπίας σχετικά με τις κινήσεις των τιμών των κρυπτονομισμάτων μέσω ενός λογαριασμού συναλλαγών CFD ή της αγοράς και πώλησης των υποκείμενων νομισμάτων μέσω ενός ανταλλακτηρίου.

Οι αγορές κρυπτονομισμάτων είναι αποκεντρωμένες, πράγμα που σημαίνει ότι δεν εκδίδονται ή δεν υποστηρίζονται από καμία κεντρική αρχή, όπως είναι μια κυβέρνηση. Αντίθετα, τρέχουν σε ένα δίκτυο υπολογιστών. Ωστόσο, τα κρυπτονομίσματα μπορούν να αγοραστούν και να πωληθούν μέσω ανταλλακτηρίων και να αποθηκευτούν σε «πορτοφόλια».

Σε αντίθεση με τα παραδοσιακά νομίσματα, τα κρυπτονομίσματα υπάρχουν μόνο ως ένα κοινό ψηφιακό αρχείο ιδιοκτησίας, αποθηκευμένο σε μια αλυσίδα μπλοκ. Όταν ένας χρήστης θέλει να στείλει κρυπτονομίσματα σε έναν άλλον χρήστη, το στέλνει στο ψηφιακό πορτοφόλι αυτού του χρήστη. Η συναλλαγή δεν θεωρείται οριστική έως ότου επαληθευτεί και προστεθεί στο blockchain μέσω της διαδικασίας της εξόρυξης. Αυτός είναι επίσης ο τρόπος με τον οποίο δημιουργούνται συνήθως νέα tokens κρυπτονομισμάτων.

Η εξόρυξη κρυπτονομισμάτων είναι η διαδικασία με την οποία ελέγχονται οι πρόσφατες συναλλαγές κρυπτονομισμάτων και προστίθενται νέα μπλοκ στο blockchain. Οι υπολογιστές εξόρυξης επιλέγουν εκκρεμείς συναλλαγές από μια ομάδα και ελέγχουν ότι ο αποστολέας έχει επαρκή χρήματα για να ολοκληρώσει τη συναλλαγή καθώς και αν η συναλλαγή πραγματοποιήθηκε χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα.

Οι μετοχές και τα κρυπτονομίσματα είναι αρκετά διαφορετικά επενδυτικά περιουσιακά στοιχεία. Ενώ και τα δύο είναι γενικά ρευστά περιουσιακά στοιχεία που ανήκουν στην κερδοσκοπική πλευρά ενός χαρτοφυλακίου, οι ομοιότητες τελειώνουν εκεί. Είναι πολύ διαφορετικοί τύποι τίτλων και ανήκουν σε πολύ διαφορετικά μέρη του χαρτοφυλακίου. Ακολουθεί μια περίληψη αυτών των δύο τύπων τίτλων.

Οι μετοχές αντιπροσωπεύουν ιδιοκτησία σε μια εισηγμένη εταιρεία. Κάθε μετοχή που αγοράζεται παρέχει ένα ποσοστό ιδιοκτησίας στην ίδια την εταιρεία. Η ιδιοκτησία αυτή λαμβάνετε ανάλογα με τον αριθμό των μετοχών που έχει εκδώσει μια εταιρεία.

Για παράδειγμα, ας πούμε ότι η XYZ Corp. απελευθερώνει το 50% της ιδιοκτησίας της με τη μορφή 50 μετοχών. Εάν αγοραστεί μία από αυτές τις μετοχές από έναν επενδυτή, θα κατέχει κυριολεκτικά το 1% της XYZ Corp. (Αν και είναι ασυνήθιστο, όταν μια εταιρεία έχει αποδεσμεύσει περισσότερο από το ήμισυ της ιδιοκτησίας της στην μορφή μετοχών, είναι δυνατό να αποκτήσει κανείς την εταιρεία απλώς αγοράζοντας αρκετές μετοχές.)

Όσων αφορά τις μετοχές, ο επενδυτής μπορεί να κερδίσει χρήματα πουλώντας τις μετοχές του σε άλλους επενδυτές. Αυτό είναι γνωστό ως capital gain, η διαφορά μεταξύ αυτού που πληρώθηκε για το περιουσιακό στοιχείο και αυτού που λήφθηκε από την πώλησή του. Πέρα από αυτό, τα οφέλη που θα αποκομιστούν από την κατοχή μετοχών εξαρτώνται αποκλειστικά από τη μεμονωμένη εταιρεία που εμπλέκεται. Οι μετοχές μπορούν επίσης να αποκτήσουν αξία πληρώνοντας μερίσματα στους επενδυτές τους, μέσω της δύναμης της ψήφου που κατέχουν οι μέτοχοι και από άλλα δικαιώματα ιδιοκτησίας. Κάθε μεμονωμένη εταιρεία είναι διαφορετική ως προς τον τρόπο που χειρίζεται ή εάν χειρίζεται ζητήματα, όπως τα μερίσματα και τα δικαιώματα ψήφου των μετόχων.

Ένα κρυπτονόμισμα είναι ένα καθαρά ψηφιακό περιουσιακό στοιχείο. Αυτό σημαίνει ότι δεν έχει φυσικό στοιχείο, αλλά υπάρχει μόνο ως καταχωρήσεις σε μια ηλεκτρονική ιδιοκτησία εγγραφής. Αυτό έρχεται σε αντίθεση με το δολάριο ΗΠΑ που έχει και ένα φυσικό στοιχείο (είναι δυνατό να γίνει ανάληψη και να κρατηθεί ένας λογαριασμός ενός δολαρίου) και ένα ψηφιακό στοιχείο (υπάρχει δυνατότητα κατοχής ενός δολαρίου σαν τίποτα

περισσότερο από μια καταχώρηση στον τραπεζικό λογαριασμό που καταγράφει αυτήν την ιδιοκτησία). Η μεμονωμένη μονάδα ενός κρυπτονομίσματος ονομάζεται token, με τον ίδιο τρόπο που η μεμονωμένη μονάδα μιας μετοχής ονομάζεται μετοχή.

Τα κρυπτονομίσματα κατηγοριοποιούνται σε δύο κύρια μέρη. Ορισμένα, όπως το γνωστό Bitcoin, προορίζονται ως καθαρά νομίσματα. Υπάρχουν μόνο για να εμπορεύονται, να αγοράζουν και να πουλάνε οι άνθρωποι. Άλλα, όπως το Ethereum, ανήκουν στην κατηγορία των "utility tokens". Αυτά τα νομίσματα λειτουργούν ως μέρος ενός πιο σύνθετου τμήματος λογισμικού, αν και παρόλα αυτά, τα utility tokens όπως το bitcoin, προορίζονται επίσης για αγοραπωλησία και διαπραγματεύσεις. Αυτήν την στιγμή υπάρχουν πολλών χιλιάδων διαφορετικών τύπων κρυπτονομισμάτων που ανταλλάσσονται παγκοσμίως.

Οι αγορές κρυπτονομισμάτων κινούνται ανάλογα με την προσφορά και τη ζήτηση. Ωστόσο, καθώς είναι αποκεντρωμένα, τείνουν να παραμένουν απαλλαγμένα από πολλές οικονομικές και πολιτικές ανησυχίες που επηρεάζουν τα παραδοσιακά νομίσματα. Ενώ εξακολουθεί να υπάρχει μεγάλη αβεβαιότητα σχετικά με τα κρυπτονομίσματα, οι ακόλουθοι παράγοντες μπορεί να έχουν σημαντικό αντίκτυπο στις τιμές τους: η προμήθεια, δηλαδή πόσο μπορεί ένα κρυπτονόμισμα να εξοριστεί, η κεφαλαιοποίηση της αγοράς(market capitalization- είναι η συνολική αξία ενός κρυπτονομίσματος), ο τύπος και το πόσο μιλάει ο πληθυσμός για το κρυπτονόμισμα, η ενσωμάτωσή του νομίσματος από άλλες εταιρείες όπως της Tesla του Elon Musk που επιτρέπει στον καταναλωτή να αγοράσει ένα καινούργιο αμάξι με bitcoin αν θέλει και το roadmap του νομίσματος, δηλαδή τι στόχους έχει βάλει να πραγματοποιήσει μέσα σε μια συγκεκριμένη χρονική περίοδο.

Κάθε έμπειρος επενδυτής πρέπει να γνωρίζει ακριβώς σε τι επενδύει. Είναι σημαντική η ισοστάθμιση στους κινδύνους και στα οφέλη της επένδυσης και τι θα οδηγήσει στην επιτυχία της επένδυσης. Εάν δεν υπάρχουν αυτού του είδους τις πληροφορίες, δεν μπορεί να γίνει κάποιος προϋπολογισμός των ρίσκων. Σε αυτήν την περίπτωση, δεν είναι πραγματικά επένδυση αλλά τζόγος.

Η επένδυση σε κρυπτονομίσματα θεωρείτε από πολλούς ως καθαρός τζόγος εφόσον δεν υπάρχει κάτι υπαρκτό όπου θα γίνει η επένδυση αλλά έχει και πολύ υψηλό ρίσκο καθώς είναι πολλοί που δημιουργούν το νόμισμά τους και το καταστρέφουν παίρνοντας όλες τις επενδύσεις των επενδυτών, τα λεγόμενα rag pulls.

Ένα πρόσφατο μεγάλο rag pull ήταν το token με την ονομασία squid game εμπνευσμένο από την τηλεοπτική σειρά με το ίδιο όνομα. Το token είχε την μορφή παιχνιδιού και οποιοσδήποτε μπορούσε να το παίξει αγοράζοντας Squid game tokens χωρίς να υπάρχει η δυνατότητα ανάληψης και μετατροπής του token σε ένα άλλο token που γίνεται εύκολα δολάριο/ευρώ. Οι δημιουργοί του εν λόγο token έφυγαν με περίπου 3.3 εκατομμύρια δολάρια μηδενίζοντας σχεδόν την αξία του token.[7]

3.6. Centralization/Decentralization

Στις παλιότερες εποχές των υπολογιστών που βασίζονταν σε mainframe, δεν υπήρχαν πολλές διαθέσιμες επιλογές όταν επρόκειτο για την κατασκευή ενός δικτύου. Ωστόσο, οι σημερινοί οργανισμοί, έχουν μια πληθώρα από επιλογές στην διάθεσή τους, επιτρέποντάς τους την κατασκευή ενός μοναδικού δικτύου που είναι συμβατό με αυτό που αναζητούν. Μια από τις σημαντικότερες αποφάσεις που πρέπει να πάρουν όμως, είναι αν θέλουν το δίκτυό τους να είναι αποκεντρωμένο ή όχι.

Η κύρια διαφορά μεταξύ αποκεντρωμένων δικτύων και μη είναι ποιος θα μπορεί να ελέγχει το δίκτυο. Σε ένα κεντρικό σύστημα, τον έλεγχο τον έχει ένα άτομο σε όλες τις πτυχές του δικτύου. Η εξουσία αυτή, συνήθως ασκείτε μέσα από ένα κεντρικό server ο οποίος διαχειρίζεται όλα τα δεδομένα και τα δικαιώματα. Ένα κεντρικό δίκτυο έχει επίσης την μεγαλύτερη του επεξεργαστική ισχύ σε εκείνον τον server.

Τα αποκεντρωμένα δίκτυα οργανώνονται με έναν πολύ πιο κατανεμημένο τρόπο. Κάθε κόμβος του δικτύου λειτουργεί ως μια ξεχωριστή οντότητα και παίρνει ανεξάρτητες αποφάσεις όσον αφορά την αλληλεπίδραση με τα υπόλοιπα συστήματα. Αυτά τα δίκτυα διανέμουν επίσης επεξεργαστική ισχύ και φόρτο εργασίας μεταξύ των συνδεδεμένων server.

Τα κεντρικά δίκτυα από την άλλη, δεδομένου ότι παρέχουν πιο άμεσο έλεγχο και είναι γενικά πιο εύκολο να ρυθμιστούν και να διαχειριστούν, πολλοί οργανισμοί εξακολουθούν να τα προτιμούν. Αυτά τα δίκτυα είναι βασισμένα γύρο από έναν κεντρικό server ο οποίος διαχειρίζεται την ισχύ, την αποθήκευση και των αδειών που είναι διαθέσιμες στους χρήστες.

Οι κεντρικοί διακομιστές υπολογιστών, τείνουν να είναι πολύ ισχυρές μηχανές που μπορούν να ανταποκρίνονται σε μεγάλο όγκο αιτημάτων από συνδεδεμένα συστήματα ενώ διαχειρίζονται και το ποιος θα έχει πρόσβαση και σε ποιους πόρους, πότε θα τους επιτραπεί η πρόσβαση και υπό ποιες προϋποθέσεις.

Η αποδοτικότητα είναι το κύριο πλεονέκτημα σε ένα τέτοιου είδους δικτύου αρχιτεκτονικής. Εφόσον όλες οι λειτουργίες ενός δικτύου διαχειρίζονται από μια κεντρική τοποθεσία, το προσωπικό του IT μπορεί να συγκεντρωθεί σε αυτούς τους server και να τους κρατάει ενημερωμένους στο λογισμικό και στο hardware.

Η κεντρική αρχιτεκτονική κάνει πιο εύκολη την παροχή μιας συνεπούς εμπειρίας στον χρήστη, επειδή το περιβάλλον του δικτύου είναι σταθερό και προβλέψιμο. Επίσης επειδή όλες οι συνδέσεις πρέπει να περάσουν από έναν κύριο server, τα αιτήματα και τα πακέτα δεδομένων συνήθως ακολουθούν την μικρότερη δυνατή διαδρομή για να φτάσουν στους στόχους τους, πράγμα που βελτιώνει την ταχύτητα και την απόδοση.

Τα αρνητικά ωστόσο των κεντρικών δικτύων είναι ότι δεν είναι πολύ ανεκτικά στα σφάλματα. Όλα τα δεδομένα πρέπει να περάσουν από μια συγκεκριμένη τοποθεσία, οπότε αν αυτή η τοποθεσία “πέσει”, είναι πολύ πιθανό να καταρρεύσει όλο το σύστημα. Αυτό κάνει τα κεντρικά δίκτυα ιδανικά για επιθέσεις, διότι μια επίθεση θα μπορούσε να θέσει σε κίνδυνο

όλα τα δεδομένα και τις εφαρμογές που βρίσκονται αποθηκευμένα εκεί. Και ενώ τα κεντρικά δίκτυα είναι καλύτερα στην αποτελεσματικότητα, μπορεί να τα οδηγήσει σε τεράστια επιβράδυνση εάν το δίκτυο δεν έχει επαρκές bandwidth για να χειριστεί την δραστηριότητα των χρηστών της.

Καθώς η επεξεργαστική ισχύ των διαφόρων μεμονωμένων συσκευών που διανέμονται στο δίκτυο έχει αυξηθεί, η αποκεντρωμένη αρχιτεκτονική έχει γίνει πιο ελκυστική. Ενώ υπάρχουν διαφορετικοί βαθμοί αποκέντρωσης, η βασική αρχή περιλαμβάνει διάφορες ανεξάρτητες μηχανές, οι οποίες συνδέονται και παρέχουν τους πόρους. Εφόσον κάθε κόμβος μέσα στο δίκτυο διατηρεί ανεξάρτητο έλεγχο, κάθε ένας από αυτούς μπορεί να δημιουργήσουν τους δικούς τους κανόνες που αφορούν τα δεδομένα και τον φόρτο εργασίας.

Η διαχείριση όλων αυτών των περίπλοκων πόρων μπορεί να είναι δύσκολη, αλλά οι αποκεντρωμένες αρχιτεκτονικές το κατέστησαν δυνατό για τους οργανισμούς να χρησιμοποιούν υπολογιστές και να αναπτύξουν μια πληθώρα συσκευών των Internet of things(IOT) με συναρπαστικούς τρόπους. Η κλιμάκωση ενός δικτύου είναι επίσης πιο εύκολη επειδή προσθέτοντας μια νέα συσκευή, αυξάνονται οι υπολογιστικοί πόροι. [25, 7]

3.6.1. Decentralized Exchange

Ένα Decentralized Exchange(Dex) είναι μια αγορά που ανταλλάσσονται κυρίως κρυπτονομίσματα. Σε ένα dex, η τεχνολογία επιτρέπει στους επενδυτές να πραγματοποιούν μεταξύ τους τις συναλλαγές αντί να χρησιμοποιούν έναν middleman όπως είναι ένα χρηματιστήριο. Οι εικονικές αγορές που χρησιμοποιούν αποκεντρωμένα συναλλάγματα όπως τα κρυπτονομίσματα είναι παραδείγματα χρήσης ενός Dex.

Ένα Dex, χρησιμοποιεί διάφορες ψηφιακές συσκευές και παρουσιάζει τις προσφορές ή την ζήτηση μιας προσφοράς ζωντανά εκείνη την στιγμή. Με αυτόν τον τρόπο, οι αγοραστές και οι πωλητές, δεν χρειάζονται να βρίσκονται ταυτόχρονα στο ίδιο σημείο για να συναλλάσουν μεταξύ τους.

Τα Dexes χρησιμοποιούν ψηφιακή τεχνολογία που επιτρέπει στους αγοραστές και στους πωλητές την ασφάλεια για να γίνονται οι συναλλαγές απευθείας μεταξύ τους. Ένα παράδειγμα της χρήσης ενός dex είναι η πώληση και η αγορά ακίνητης περιουσίας όπου ο αγοραστής επικοινωνεί απευθείας με τον πωλητή. Ένα πιο σύγχρονο παράδειγμα είναι οι εικονικές αγορές και το σύστημα του Blockchain που χρησιμοποιούν κρυπτονομίσματα.

Ένα παράδειγμα ενός Dex είναι η αγορά συναλλάγματος(forex market) όπου η αγοραπωλησία περιέχει παγκόσμια νομίσματα(ευρώ, δολάριο, γεν κ.α.) επειδή η αγοραπωλησία δεν γίνεται σε ένα φυσικό μέρος. Οι χρήστες του forex χρησιμοποιούν το διαδίκτυο για να ελέγξουν τις τιμές των χρημάτων που παρέχουν διάφοροι αντιπρόσωποι στον κόσμο.

Η ακίνητη περιουσία είναι άλλο ένα παράδειγμα για την χρήση των dex. Η ακίνητη περιουσία πωλείται παραδοσιακά μέσω μιας αποκεντρωμένης αγοράς, όπου οι αγοραστές και

οι πωλητές ολοκληρώνουν τις συναλλαγές τους χωρίς μια πρώτη διοχέτευση διαδικασίας ενός μεσάζοντα. Ορισμένα ομόλογα αλλά και προϊόντα μπορούν επίσης να πωληθούν και τα ίδια στην αποκεντρωμένη αγορά.

Η χρήση της τεχνολογίας του Blockchain και των κρυπτονομισμάτων, έχουν δημιουργήσει ευκαιρίες που οι αποκεντρωμένες αγορές μπορούν να εκμεταλλευτούν για την λειτουργία τους. Συνήθως οι εικονικές αγορές δεν ρυθμίζονται από κάποια αρχή όπως είναι το κράτος και αυτό πιστεύουν οι υποστηρικτές της ότι είναι κάτι καλό. Η τεχνολογία και τα μέσα όπως είναι τα κρυπτονομίσματα των εικονικών αγορών, παρέχουν στους επενδυτές τους, μια αίσθηση ασφάλειας και εμπιστοσύνης με τις συναλλαγές τους.

Η ανάπτυξη των αγορών που χρησιμοποιούν αποκεντρωμένα νομίσματα για τις συναλλαγές τους, οδήγησαν σε συζητήσεις σχετικά με την ρύθμισή τους. Αν συνέβαινε αυτό, οι υποστηρικτές των εικονικών αγορών, θα το έβλεπαν σαν μείωση ως προς την ανωνυμία που τους παρέχεται και στην μείωση των άμεσων ελέγχων των συναλλαγών τους.

Το αποκεντρωμένο χρήμα, τα peer-to-peer χρήματα και το ψηφιακό νόμισμα αναφέρονται στις μεθόδους που δεν χρησιμοποιούν τραπεζικούς τρόπους μεταφοράς αγαθών ή άλλων τρίτων παραγόντων. Οι περισσότερες μη αποκεντρωμένες και μερικές αποκεντρωμένες αγορές χρησιμοποιούν το νόμισμα fiat ή ρευστά νομίσματα που εκδίδονται από τις κεντρικές τράπεζες. Το αποκεντρωμένο χρήμα χρησιμοποιείται κυρίως στις εικονικές αγορές. Δύο τέτοια παραδείγματα είναι το bitcoin του δικτύου Bitcoin και το ether του Ethereum.

Πλεονεκτήματα των Dexes:

- Ορισμένοι πιστεύουν ότι με τα Dexes, θα μειωθούν σημαντικά οι επιθέσεις από χάκερ επειδή δεν υπάρχει μια κεντρική πηγή στην οποία μπορούν να διεισδύσουν αλλά αυτό δεν ισχύει.
- Οι αποκεντρωμένες αγορές είναι “διάφανες” και επιτρέπουν σε οποιονδήποτε να τις κοιτάξει ειδικά εάν χρησιμοποιούν κάποια τεχνολογία που διασφαλίζει ότι όλα τα μέρη τους μοιράζονται συμφωνημένα δεδομένα και πληροφορίες.
- Πολλοί που χρησιμοποιούν αποκεντρωμένες εικονικές αγορές αντιλαμβάνονται την έλλειψη της ρυθμιστικής επίβλεψης και την ελευθερία από μεσάζοντες ως όφελος.
- Η απουσία των διαμεσολαβητών, μπορεί να οδηγήσει σε χαμηλότερο κόστος συναλλαγής από ότι στις αγορές που υπόκεινται σε ρυθμίσεις.

Πέρα όμως από την πληθώρα πλεονεκτημάτων, τα Dexes έρχονται και με τα μειονεκτήματα τους, όπως:

- Ένα σημαντικό μειονέκτημα είναι η έλλειψη των κυβερνητικών αρχών για να παρακολουθήσουν τις συναλλαγές που γίνονται και έτσι δεν υπάρχει κάποια νόμιμη βοήθεια σε περίπτωση κλοπής ή απώλειας.

- Εφόσον όλο και περισσότερες αγορές κινούνται στις αποκεντρωμένες συναλλαγές, δημιουργούν όλο και μεγαλύτερες προκλήσεις για τις ρυθμιστικές αρχές και τις νομικές επιβολές. Για παράδειγμα, η κεντρική αγορά μπορεί να δείξει στην κυβέρνηση τον τρόπο που ενεργεί για να λάβει μέτρα, εάν είναι απαραίτητο, σχετικά με ύποπτες συναλλαγές που μπορεί να έχουν λάβει μέρος.[3, 26]

4. Η ΕΞΕΛΙΞΗ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

4.1. Web1.0

Το Web 1.0 ήταν η πρώτη εφαρμογή του παγκόσμιου ιστού και διήρκησε από το 1989 μέχρι το 2005. Ορίστηκε ως το δίκτυο που σύνδεε τις πληροφορίες. Σύμφωνα με τον δημιουργό του διαδικτύου, τον Tim Berners-Lee θεωρούσε ότι το διαδίκτυο ότι ήταν read-only και έχει πολύ μικρή αλληλεπίδραση με τον χρήστη όπου ο χρήστης μπορεί να ανταλλάξει πληροφορίες αλλά δεν μπορούσε να αλληλοεπιδράσει με τους ιστότοπους. Ο ρόλος του ιστού έπαιζε έναν πολύ παθητικό ρόλο.

Το Web 1.0 αναφέρεται ως η πρώτη γενιά του διαδικτύου και χαρακτηρίστηκε ως “ένας χώρος πληροφοριών του οποίου τα στοιχεία του αναφέρονται ως πόροι καλούμενοι Uniform Resources Identifiers (URIs)”. Η πρώτη περίοδος του διαδικτύου ήταν στατική και το περιεχόμενό του ήταν μόνο επί του σκοπού της παράδοσης. Με λίγα λόγια, στον πρώιμο ιστό μπορούσαμε μόνο να αναζητήσουμε πληροφορίες και να τις διαβάσουμε. Ο χρήστης δεν είχε σχεδόν καμία αλληλεπίδραση με την ιστοσελίδα.

Το Web 1.0 περιλάμβανε τα πρωτόκολλα της HTTP, HTML και του URL. Τα σημαντικότερα χαρακτηριστικά αυτού του πρώιμου ιστού ήταν:

- Το περιεχόμενό του δεν μπορούσε να επεξεργαστεί.
- Η δημιουργία μιας διαδικτυακής παρουσίας και την ικανότητα να διαθέτει τις πληροφορίες οπουδήποτε στον κάθε έναν.
- Περιλάμβανε στατικές ιστοσελίδες και χρησιμοποιούσε την HTML(HyperText Markup Language) γλώσσα.

Οι περιορισμοί του Web 1.0 ήταν πολλοί συμπεριλαμβανομένου και των παρακάτω:

- Οι ιστοσελίδες κατανοούνταν μόνο από τους ανθρώπους και δεν ήταν συμβατές με άλλα μηχανήματα.
- Ο λεγόμενος webmaster ήταν υπεύθυνος για την αναβάθμιση χρηστών και την επεξεργασία του περιεχομένου της ιστοσελίδας.
- Ήταν αδύνατη η χρήση της δυναμικής αναπαράστασης αφού όλες οι σελίδες ήταν στατικές και καμία ιστοσελίδα δεν μπορούσε να εκτελέσει δυναμικά συμβάντα.[28,41]

4.2. Web 2.0

Ως Web 2.0 χαρακτηρίζεται η δεύτερη γενιά του διαδικτύου. Ορίστηκε από τον Dale Dougherty σαν ένα διαδίκτυο τύπου ανάγνωσης-γραφής. Η ιδέα ξεκίνησε σε μια συνεδρία

ανάμεσα στον O'Reilly και στο Media live International. Οι τεχνολογίες του Web 2.0 επιτρέπουν την συγκέντρωση και την διαχείριση ενός μεγάλου ανθρώπινου ποσοστού που μοιράζονται κοινά ενδιαφέροντα και έχουν ίδιες κοινωνικές αλληλεπιδράσεις.

Ο Tim O'Reilly όρισε το Web 2.0 στην ιστοσελίδα του ως εξής: "Το Web 2.0 είναι μια επιχειρηματική επανάσταση στη βιομηχανία των υπολογιστών που προκλήθηκε από τη μετάβαση στο διαδίκτυο ως πλατφόρμα και μια προσπάθεια κατανόησης των κανόνων επιτυχίας σε αυτήν τη νέα πλατφόρμα. Ο κύριος μεταξύ αυτών των κανόνων είναι ο εξής: Η δημιουργία εφαρμογών που αξιοποιούν το δίκτυο για να βελτιώνεται όσο περισσότεροι άνθρωποι τις χρησιμοποιούν."

Το Web 2.0 φιλοξενεί πολλές ιδιότητες μερικές των οποίων είναι και η συμμετοχική ικανότητα, η δυνατότητα συνεργασίας και οι κατανεμημένες πρακτικές που επιτρέπουν επίσημες και άτυπες δραστηριότητες καθημερινά στο διαδίκτυο. Με άλλα λόγια αντιπροσωπεύει ένα μεγάλο διακριτό χαρακτηριστικών του Web 2.0 συμπεριλαμβανομένου και των σχεσιακών τεχνολογιών μέσα σε μια κοινωνική ψηφιακή τεχνολογία που μπορεί να οριστεί και ως το δίκτυο της σοφίας. Ο ανθρωποκεντρικός ιστός και ο συμμετοχικός ιστός λαμβάνουν υπόψη και ποιες διευκολύνσεις ανάγνωσης και εγγραφής στον ιστό καθιστούν τη συναλλαγή αμφίδρομη.

Το Web 2.0 είναι μια πλατφόρμα ιστού όπου οι χρήστες μπορούν να αφήσουν πολλούς ελέγχους. Με άλλα λόγια ένας χρήστης του Web 2.0 έχει μεγαλύτερη αλληλεπίδραση και λιγότερο έλεγχο. Το Web 2.0 δεν είναι μόνο μια καινούργια έκδοση του Web 1.0 αλλά έχει και ευέλικτο σχεδιασμό ιστοσελίδων, δημιουργική επαναχρησιμοποίηση, ενημερώσεις, την συλλογική δημιουργία περιεχομένου και την τροποποίηση στο Web 2.0. Αυτό το οποίο πρέπει να θεωρηθεί ως ένα από τα εξαιρετικά χαρακτηριστικά του Web 2.0 είναι η υποστήριξη της συνεργασίας και η βοήθεια της συλλογικής νοημοσύνης.

Το Web 2.0 μπορεί να κατανοηθεί καλύτερα με τους παρακάτω ορισμούς:

- Τεχνολογικός ορισμός: το διαδίκτυο έχει γίνει μια πλατφόρμα με λογισμικό πάνω από μιας μεμονωμένης συσκευής. Η τεχνολογία σχετίζεται με την ιστολογία, τα wiki, τα podcasts, το RSS FEED και άλλα πολλά.
- Επιχειρηματικός ορισμός: Ένας τρόπος αρχιτεκτονικής λογισμικού και επιχειρήσεων. Η επιχειρηματική επανάσταση στη βιομηχανία των υπολογιστών προκλήθηκε από τη μετάβαση στο διαδίκτυο ως πλατφόρμα και μια προσπάθεια κατανόησης των κανόνων επιτυχίας σε αυτήν της νέας πλατφόρμας.
- Χρηστικός ορισμός: Ο κοινωνικός ιστός χρησιμοποιείται συχνά για τον χαρακτηρισμό ιστοτόπων που αποτελούνται από κοινότητες. Όλα είναι σχετικά με τη διαχείριση περιεχομένου και τους νέους τρόπους επικοινωνίας και αλληλεπίδρασης μεταξύ των χρηστών. Οι εφαρμογές ιστού διευκολύνουν τη συλλογική παραγωγή γνώσης και την κοινωνική δικτύωση καθώς αυξάνουν την ανταλλαγή πληροφοριών μεταξύ χρηστών.

Μερικές φορές, εάν η νέα τεχνολογία ανταποκριθεί θετικά στις προσδοκίες των περισσοτέρων, υπάρχει περίπτωση η τεχνολογία αυτή να έρθει αντιμέτωπη με πολλές συνέπιες από εξωτερικούς παράγοντες οι οποίοι μπορεί να περιορίσουν την ροή της παρουσιάζοντας αποτελέσματα που μπορεί να μην είναι εφικτά και μπορεί να οδηγήσουν στην υποβάθμιση της απόδοσης της τεχνολογίας στο σύνολό της όπως είναι τα παρακάτω:

- Κύκλος συνεχούς επανάληψης Αλλαγών και Ενημερώσεων στις υπηρεσίες.
- Δεοντολογικά ζητήματα που αφορούν την κατασκευή και τη χρήση του Web 2.0.
- Διασυνδεσιμότητα και ανταλλαγή γνώσεων μεταξύ πλατφορμών πέρα από τα όρια της κοινότητας να έχουν περιορισμούς. [28,41]

4.3. Web 3.0

Το Web 3.0 είναι ένα από τα σύγχρονα και εξελικτικά θέματα που σχετίζονται με τις ακόλουθες πρωτοβουλίες του Web 2.0. Το Web 3.0 επινοήθηκε για πρώτη φορά από τον John Markoff των New York Times και πρότεινε το Web 3.0 ως τρίτη γενιά του Ιστού το 2006. Το Web 3.0 μπορεί επίσης να δηλωθεί ως το "εκτελέσιμο Web".

Η βασική ιδέα του Web 3.0 είναι να ορίσει δεδομένα δομής και να τα συνδέσει με σκοπό την αποτελεσματικότερη ανακάλυψη, αυτοματοποίηση, ενοποίηση και επαναχρησιμοποίηση σε διάφορες εφαρμογές. Είναι σε θέση να βελτιώσει τη διαχείριση δεδομένων, να υποστηρίξει την προσβασιμότητα στο κινητό Διαδίκτυο, να προσομοιώσει την δημιουργικότητα και την καινοτομία, να ενθαρρύνει τα φαινόμενα παγκοσμιοποίησης, να ενισχύσει την ικανοποίηση των πελατών και να βοηθήσει στην οργάνωση της συνεργασίας στον κοινωνικό ιστό.

Το Web 3.0 είναι επίσης γνωστό ως ο σημασιολογικός ιστός. Ο σημασιολογικός ιστός δημιουργήθηκε από τον Tim Berners-Lee, εφευρέτη του World Wide Web. Υπάρχει μια ειδική ομάδα στην κοινοπραξία του Παγκόσμιου Ιστού (W3C) που εργάζεται για τη βελτίωση, την επέκταση και την τυποποίηση του συστήματος. Οι γλώσσες, οι δημοσιεύσεις και τα εργαλεία έχουν ήδη αναπτυχθεί. Το Web 3.0 είναι ένας ιστός όπου η έννοια του ιστότοπου ή της ιστοσελίδας εξαφανίζεται, τα δεδομένα δεν ανήκουν στην ιδιοκτησία αλλά αντ' αυτού κοινοποιούνται και οι υπηρεσίες εμφανίζουν διαφορετικές προβολές για τον ίδιο ιστό ή τα ίδια δεδομένα. Αυτές οι υπηρεσίες μπορεί να είναι εφαρμογές (όπως προγράμματα περιήγησης, εικονικοί κόσμοι ή οτιδήποτε άλλο), συσκευές ή άλλες, και πρέπει να εστιάζονται στο περιβάλλον και την εξατομίκευση και θα προσεγγιστούν και οι δύο με τη χρήση της κάθετης αναζήτησης.

Το Web 3.0 υποστηρίζει παγκόσμια βάση δεδομένων και έχει αρχιτεκτονική γύρο από τον ιστό η οποία στα πρώιμα στάδιά της περιγραφόταν ως ένας ιστός εγγράφων. Ασχολείται κυρίως με στατικά HTML έγγραφα αλλά και με σελίδες που αποδίδουν δυναμικά και με εναλλακτικές μορφές που πρέπει να ακολουθούν τα ίδια πρότυπα εννοιολογικής διάταξης όποτε είναι δυνατόν και οι σύνδεσμοι να βρίσκονται μεταξύ εγγράφων ή μέρους τους. Ο ιστός των εγγράφων σχεδιάστηκε για την ανθρώπινη κατανάλωση, στον οποίο τα κύρια αντικείμενα

είναι έγγραφα και οι σύνδεσμοι μεταξύ των εγγράφων (ή τμημάτων τους). Η σημασιολογία του περιεχομένου και των συνδέσμων είναι σιωπηρή και ο βαθμός δομής μεταξύ των αντικειμένων είναι αρκετά χαμηλός.

Οι υποστηρικτές του Web of Data οραματίζονται πολλά από τα δεδομένα του κόσμου να είναι αλληλένδετα και προσβάσιμα στο ευρύ κοινό. Αυτό το όραμα είναι αναλογικό από πολλές απόψεις αλλά αντί να γίνονται ανοιχτά προσβάσιμα τα έγγραφα και τα μέσα, η εστίαση είναι στο να είναι ανοιχτή η πρόσβαση στα δεδομένα. Το Web of Data φιλοξενεί μια ποικιλία συνόλων δεδομένων που περιλαμβάνουν εγκυκλοπαιδικά γεγονότα, δεδομένα φαρμάκων και πρωτεϊνών, μεταδεδομένα για μουσική, βιβλία και επιστημονικά άρθρα, αναπαραστάσεις κοινωνικών δικτύων, γεωχωρικές πληροφορίες και πολλά άλλα είδη πληροφοριών κατά κάποιο τρόπο όπως είναι μια παγκόσμια βάση δεδομένων που περιλαμβάνονται τα περισσότερα χαρακτηριστικά της. Η σημασιολογία του περιεχομένου και των συνδέσμων είναι σαφής και ο βαθμός της δομής μεταξύ των αντικειμένων είναι υψηλός με βάση το μοντέλο RDF.

Ο Σημασιολογικός Ιστός είναι ένα κίνημα συνεργασίας με επικεφαλή τον οργανισμό διεθνών προτύπων, την Κοινοπραξία του Παγκόσμιου Ιστού. Σύμφωνα με το W3C, «Ο Σημασιολογικός Ιστός παρέχει ένα κοινό πλαίσιο που επιτρέπει την κοινή χρήση και επαναχρησιμοποίηση δεδομένων μεταξύ των ορίων εφαρμογών, επιχειρήσεων και κοινότητας».

Ο κύριος σκοπός του Σημασιολογικού Ιστού είναι να οδηγήσει την εξέλιξη του τρέχοντος Ιστού δίνοντας τη δυνατότητα στους χρήστες να βρίσκουν, να μοιράζονται και να συνδυάζουν σχηματισμούς πιο εύκολα. Ο Σημασιολογικός Ιστός, όπως είχε αρχικά οραματιστεί, είναι ένα σύστημα που επιτρέπει στις μηχανές να «κατανοούν» και να ανταποκρίνονται σε περίπλοκα ανθρώπινα αιτήματα με βάση το νόημά τους. Μια τέτοια «κατανόηση» απαιτεί οι σχετικές πηγές πληροφοριών να είναι σημασιολογικά δομημένες.

Ο Tim Berners-Lee εξέφρασε αρχικά τον Σημασιολογικό Ιστό ως εξής: «Εάν η HTML και ο Ιστός έκαναν όλα τα διαδικτυακά έγγραφα να μοιάζουν με ένα τεράστιο βιβλίο, τα σχήματα RDF θα κάνουν όλα τα δεδομένα στον κόσμο να μοιάζουν με μια τεράστια βάση δεδομένων».

Ο σημασιολογικός ιστός δεν περιορίζεται στη δημοσίευση δεδομένων στο διαδίκτυο. Πρόκειται για τη δημιουργία συνδέσμων όπου συνδέουν σχετικά δεδομένα. Ο Berners-Lee εισήγαγε ένα σύνολο κανόνων που έγιναν γνωστοί ως οι αρχές Συνδεδεμένων Δεδομένων για τη δημοσίευση και τη σύνδεση δεδομένων στον Ιστό το 2007:

- Η χρήση των URI για την ονομασία πραγμάτων.
- Η χρήση των HTTP URI για την εύρεση αυτών των ονομάτων.
- Η παροχή χρήσιμων πληροφοριών χρησιμοποιώντας πρότυπα(URI) για την εύρεση ενός URI.

- Η συμπερίληψη υπερσυνδέσμων για άλλα URI με σκοπό την εύρεση περισσότερων πραγμάτων.

Οι πάροχοι δεδομένων μπορούν να προσθέσουν τα δεδομένα τους σε έναν ενιαίο παγκόσμιο χώρο δεδομένων δημοσιεύοντας δεδομένα στο διαδίκτυο σύμφωνα με τις αρχές των Συνδεδεμένων Δεδομένων.

Τα κυριότερα χαρακτηρίστηκα του Web 3.0 όπως επισημαίνονται από τον Nova Spivac είναι τα εξής:

- Το επιχειρηματικό του μοντέλο SaaS.
- Η πλατφόρμα λογισμικού ανοιχτού κώδικα.
- Η κατανεμημένη βάση δεδομένων – ή αυτό που ονομάζεται «Η παγκόσμια βάση δεδομένων».
- Η εξατομίκευση διαδικτύου.
- Η συγκέντρωση πόρων.
- Το έξυπνο διαδίκτυο.

Μερικές από τις προκλήσεις που αντιμετωπίζει ο σημασιολογικός ιστός είναι οι παρακάτω:

- Το μέγεθος: Το διαδίκτυο περιέχει πολλά δισεκατομμύρια σελίδες. Ενδέχεται να προκύψει πλεονασμός των δεδομένων αν δεν έχει ακόμη καταφέρει να εξαλείψει όλους τους σημασιολογικά διπλότυπους όρους.
- Η αοριστία: Αυτό προκύπτει από την ασάφεια των ερωτημάτων των χρηστών, των εννοιών που αντιπροσωπεύονται από τους παρόχους περιεχομένου, της αντιστοίχισης όρων ερωτήματος με όρους παρόχου και της προσπάθειας συνδυασμού διαφορετικών βάσεων γνώσης με επικαλυπτόμενες αλλά διακριτικά διαφορετικές έννοιες.
- Η ασυνέπεια: Πρόκειται για λογικές αντιφάσεις που αναπόφευκτα προκύπτουν κατά την ανάπτυξη μεγάλων οντολογιών και όταν συνδυάζονται οντολογίες από ξεχωριστές πηγές.
- Ο δόλος: Αυτό συμβαίνει όταν ο παραγωγός των πληροφοριών παραπλανά σκόπιμα τον καταναλωτή.

Η κύρια διαφορά μεταξύ Web 1.0, Web 2.0 και Web 3.0 είναι ότι το Web 1.0 θεωρείται μόνο για ανάγνωση. Ο στόχος του Web 1.0 είναι στη δημιουργικότητα περιεχομένου του παραγωγού. Το Web 2.0 στοχεύει στη δημιουργικότητα περιεχομένου των χρηστών και των παραγωγών ενώ το Web 3.0 στοχεύει σε συνδεδεμένα σύνολα δεδομένων. Οι διαφορές μεταξύ Web 1.0, Web 2.0 και Web 3.0 δίνονται παρακάτω: [28,41]

WEB 1.0	WEB 2.0	WEB 3.0
1996 – 2004	2004 -2016	2016+
The Hypertext Web	The Social Web	The Semantic Web
Tim Berners Lee	Tim O'Reilly, Dale Dougherty	Tim Berners Lee
Read Only	Read and Write Web	Executable Web
Millions of User	Billions of User	Trillions+ of Users
Echo System	Participation and Interaction	Understanding self
One Directional	Bi-Directional	Multi-user Virtual environment

Εικόνα 11: Διαφορές των Web1.0, Web 2.0, Web 3.0[41]

5. Metaverse

Το metaverse είναι μια ψηφιακή πραγματικότητα που συνδυάζει τα μέσα κοινωνικής δικτύωσης, το διαδικτυακό παιχνίδι, την επαυξημένη πραγματικότητα (AR), την εικονική πραγματικότητα (VR), τα κρυπτονομίσματα και επιτρέπει στους χρήστες να αλληλοεπιδρούν εικονικά. Η επαυξημένη πραγματικότητα καλύπτει οπτικά στοιχεία, ήχο και άλλα αισθητηριακά δεδομένα σύμφωνα με τον πραγματικό κόσμο για να βελτιώσει την εμπειρία του χρήστη. Αντίθετα, η εικονική πραγματικότητα είναι εξ ολοκλήρου εικονική.

Καθώς το metaverse μεγαλώνει, θα δημιουργήσει διαδικτυακούς χώρους όπου οι αλληλεπιδράσεις των χρηστών θα είναι πιο πολυδιάστατες από ό,τι υποστηρίζει η τρέχουσα τεχνολογία. Αντί να βλέπουν απλώς ψηφιακό περιεχόμενο, οι χρήστες στο metaverse θα βυθίζονται σε έναν χώρο όπου ο ψηφιακός και ο φυσικός κόσμος συγκλίνουν.

Το metaverse είναι ένα κοινό εικονικό περιβάλλον στο οποίο οι άνθρωποι έχουν πρόσβαση μέσω του Διαδικτύου. Τεχνολογίες όπως η εικονική πραγματικότητα (VR) και η επαυξημένη πραγματικότητα (AR) συνδυάζονται στο metaverse για να δημιουργήσουν μια αίσθηση ρεαλισμού και «εικονικής παρουσίας».

Ο διευθύνων σύμβουλος του Facebook, Mark Zuckerberg, πιστεύει ότι τα γυαλιά επαυξημένης πραγματικότητας θα είναι τελικά τόσο διαδεδομένα όσο τα smartphone.Τον Οκτώβριο του 2021, το Facebook ανακοίνωσε τα σχέδια του για τη δημιουργία 10.000 νέων θέσεων εργασίας υψηλής ειδίκευσης στην Ευρωπαϊκή Ένωση (ΕΕ) για να βοηθήσει στη διαμόρφωση του metaverse.

Η λέξη metaverse, άρχισε να εμφανίζεται δημόσια όταν άρχισαν να φουντώνουν οι φήμες στα μέσα Οκτωβρίου του 2021 σχετικά με μια μετονομασία του Facebook για να

φαίνεται σαν εταιρεία πιο σχετική με το metaverse. Ανώνυμες πηγές είπαν στην δημοσιογράφο Casey Newton ότι το Facebook θα ανακοινώσει σύντομα την μετονομασία του, όπως και μετά από λίγο, έγινε.

Ο Διευθύνων Σύμβουλος του Facebook, Mark Zuckerberg, ανακοίνωσε το νέο όνομα, Meta, στο συνέδριο Connect 2021 του Facebook στις 28 Οκτωβρίου, με τη νέα του ιστοσελίδα να το χαρακτηρίζει «εταιρία κοινωνικής τεχνολογίας». “Στο metaverse, θα μπορείτε να κάνετε σχεδόν ό,τι μπορείτε να φανταστείτε—να συναντηθείτε με φίλους και οικογένεια, να εργαστείτε, να μάθετε, να παίξετε, να ψωνίσετε, να δημιουργήσετε—καθώς και εντελώς νέες εμπειρίες που δεν ταιριάζουν πραγματικά με το πώς σκεφτόμαστε σχετικά με τους υπολογιστές ή τα τηλέφωνα σήμερα...Σε αυτό το μέλλον, θα μπορείτε να τηλεμεταφέρεστε αμέσως ως ολόγραμμα για να είστε στο γραφείο χωρίς μετακινήσεις, σε μια συναυλία με φίλους ή στο σαλόνι των γονιών σας ”, δήλωσε ο Zuckerberg σύμφωνα με το Founder's Letter του 2021, που κυκλοφόρησε στις 28 Οκτωβρίου.

"Μπορείτε να παρακολουθήσετε την πλήρη ομιλία του Connect και να μάθετε περισσότερα για το πώς το metaverse θα ξεκλειδώσει νέες ευκαιρίες στο Meta.com. Μπορείτε επίσης να μάθετε περισσότερα για τη δουλειά μας τους τελευταίους μήνες για την ανάπτυξη της επωνυμίας Meta στο ιστολόγιο σχεδιασμού μας", διαφήμισε το Meta στον ιστότοπό του. Η επιστολή του Zuckerberg διαφημίζει ότι το Meta “γύρισε μια ταινία που εξερευνά πώς μπορείς να χρησιμοποιήσεις το metaverse μια μέρα”.

Το Facebook μίλησε για το metaverse, σημειώνοντας σε ένα δελτίο τύπου στις 17 Οκτωβρίου 2021 ότι το metaverse είναι “μια νέα φάση διασυνδεδεμένων εικονικών εμπειριών που χρησιμοποιούν τεχνολογίες όπως της εικονικής και της επαυξημένης πραγματικότητας. Στην καρδιά του βρίσκεται η ιδέα ότι, δημιουργώντας μια μεγαλύτερη αίσθηση «εικονικής παρουσίας», η αλληλεπίδραση στο διαδίκτυο μπορεί να έρθει πολύ πιο κοντά στην εμπειρία της προσωπικής αλληλεπίδρασης”.

Το ενδιαφέρον για το metaverse αναμένεται να αυξηθεί σημαντικά καθώς επενδυτές και εταιρείες θέλουν να είναι μέρος αυτού που θα μπορούσε να είναι το επόμενο μεγάλο άλμα. Το metaverse “θα είναι ένα μεγάλο επίκεντρο [του Facebook] και νομίζω ότι αυτό θα είναι απλώς ένα μεγάλο μέρος του επόμενου κεφαλαίου για τον τρόπο με τον οποίο το Διαδίκτυο εξελίσσεται μετά το κινητό διαδίκτυο”, δήλωσε ο Zuckerberg στον τεχνολογικό ιστότοπο The Verge πριν ανακοινωθεί η αλλαγή του ονόματος. “Και νομίζω ότι θα είναι το επόμενο μεγάλο κεφάλαιο και για την εταιρεία μας, διπλασιάζοντας πραγματικά σε αυτόν τον τομέα”.

Οι υποστηρικτές του metaverse θεωρούν την ιδέα ως το επόμενο στάδιο στην ανάπτυξη του Διαδικτύου. Το Facebook, για παράδειγμα, έχει ήδη επενδύσει πολλά χρήματα σε AR και VR, αναπτύσσοντας υλικό όπως τα ακουστικά Oculus VR, ενώ οι τεχνολογίες οπτικών AR και περιβραχιόνιων βρίσκονται πολύ κοντά.

Ο Zuckerberg, ο οποίος πιστεύει ότι τα γυαλιά AR θα είναι κάποτε παντού όπως τα smartphone, είπε στο The Verge ότι τα επόμενα χρόνια, το Facebook “θα μεταβεί ουσιαστικά από τους ανθρώπους που μας βλέπουν κυρίως ως εταιρεία κοινωνικών μέσων μαζικής ενημέρωσης σε μια εταιρεία metaverse”.

Πολυάριθμα βιβλία επιστημονικής φαντασίας, τηλεοπτικές σειρές και ταινίες διαδραματίζονται σε metaverses – ψηφιακοί κόσμοι που δεν διακρίνονται από τον πραγματικό κόσμο. Στην πραγματικότητα, ο συγγραφέας επιστημονικής φαντασίας Neal Stephenson επινόησε τον όρο metaverse στο μυθιστόρημά του Snow Crash το 1992.

Στο βιβλίο, ανθρώπινα avatar και πράκτορες λογισμικού αλληλοεπιδρούν σε έναν τρισδιάστατο εικονικό χώρο. Συχνά, αυτά τα metaverses είναι δυστοπικοί κόσμοι. Μερικοί από τους “σύγχρονους” Zuckerberg ανησυχούν ότι το πραγματικό metaverse - το «Διαδίκτυο επόμενης γενιάς» - θα μπορούσε να γίνει ένας δυστοπικός εφιάλτης.

Ο Διευθύνων Σύμβουλος της Niantic(μια εταιρεία λογισμικού που είναι γνωστή για τα παιχνίδια Ingress και Pokémon GO), John Hanke, για παράδειγμα, έγραψε σε μια ανάρτηση στο ιστολόγιο του ότι, “Πολλοί άνθρωποι αυτές τις μέρες φαίνονται πολύ να ενδιαφέρονται να φέρουν στη ζωή αυτό το όραμα ενός εικονικού κόσμου στο άμεσο μέλλον, συμπεριλαμβανομένων μερικών από τα μεγαλύτερα ονόματα της τεχνολογίας και του gaming. Αλλά στην πραγματικότητα, αυτά τα μυθιστορήματα χρησίμευσαν ως προειδοποιήσεις για ένα δυστοπικό μέλλον της τεχνολογίας που πήγε στραβά”.

Η πανδημία του COVID-19 επιτάχυνε το ενδιαφέρον για το metaverse καθώς περισσότεροι άνθρωποι εργάζονταν από το σπίτι και πήγαιναν σχολείο εξ αποστάσεως. Φυσικά, υπάρχουν ανησυχίες ότι με το metaverse θα είναι πιο εύκολο οι άνθρωποι να περνούν χρόνο χωριστά —ακόμα και μετά τον COVID-19.

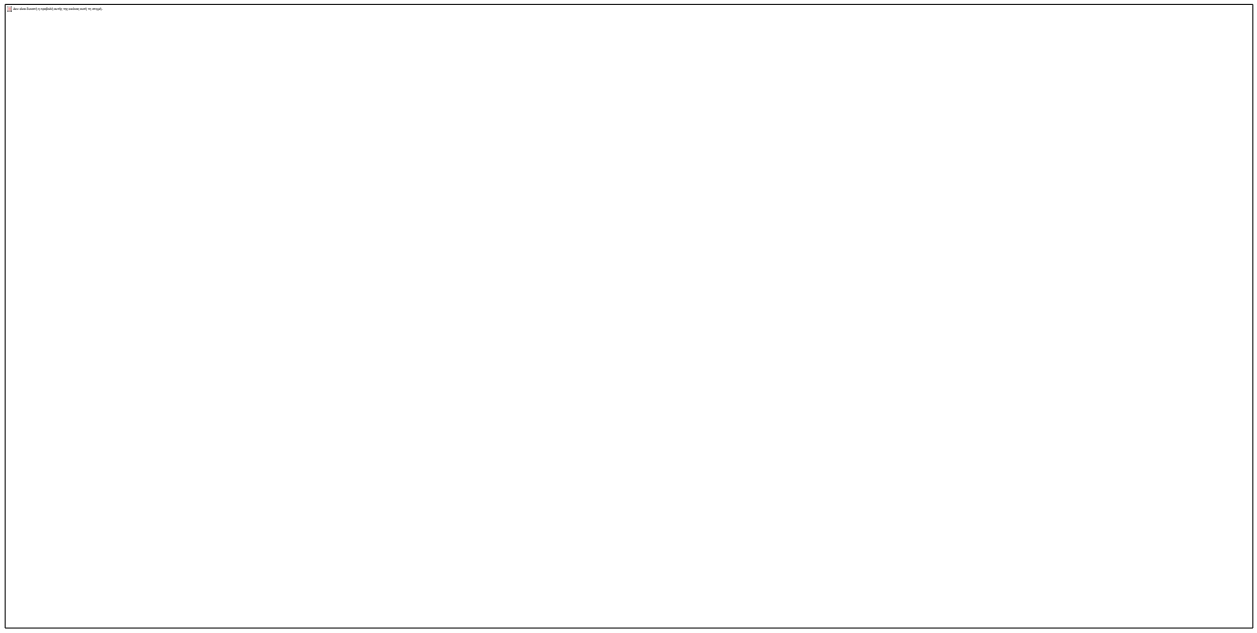
Ο Hanke έγραψε: “Πιστεύουμε ότι μπορούμε να χρησιμοποιήσουμε την τεχνολογία για να γείρουμε στην «πραγματικότητα» της επαυξημένης πραγματικότητας – ενθαρρύνοντας όλους, συμπεριλαμβανομένων των εαυτών μας, να σηκωθούν, να περπατήσουν έξω και να συνδεθούν με τους ανθρώπους και τον κόσμο γύρω μας... Η τεχνολογία πρέπει να χρησιμοποιηθεί για να βελτιώνει τις βασικές ανθρώπινες εμπειρίες - όχι να τις αντικαταστεί”.

Το Facebook ορίζει το metaverse ως “ένα σύνολο εικονικών χώρων όπου γίνεται να δημιουργηθούν και να εξερευνηθούν από πολλά άτομα που δεν βρίσκονται στον ίδιο φυσικό χώρο”. Αν και η τεχνολογία metaverse απέχει χρόνια από την πλήρη υλοποίηση της, αναμένεται τελικά να είναι ένα μέρος όπου θα υπάρχει η δυνατότητα εργασίας, παιχνιδιού, μάθησης, δημιουργίας, και αλληλεπίδρασης με φίλους σε ένα εικονικό, διαδικτυακό περιβάλλον.

Η επαυξημένη πραγματικότητα καλύπτει τα οπτικά στοιχεία, τα ηχητικά και τα στοιχεία άλλων αισθητηριακών ερεθισμάτων σε ένα πραγματικό περιβάλλον για τη βελτίωση της εμπειρίας του χρήστη. Το AR μπορεί να προσπελαστεί με ένα smartphone και οι χρήστες

μπορούν να ελέγξουν την παρουσία τους στον πραγματικό κόσμο. Συγκριτικά με την εικονική πραγματικότητα(VR), η εικονική πραγματικότητα είναι εντελώς εικονική και ενισχύει τις φανταστικές πραγματικότητες. Το VR απαιτεί συσκευή ακουστικών και οι χρήστες ελέγχονται από το σύστημα.

Το metaverse δεν έχει μοναδικό δημιουργό, επομένως δεν είναι κάτι που το Facebook κατέχει και δεν είναι αποκλειστικά υπεύθυνο για την ανάπτυξη του. Παρόλα αυτά, το Facebook έχει ήδη επενδύσει πολλά χρήματα στο metaverse μέσω των ακουστικών Oculus VR και εργάζεται σε τεχνολογίες γυαλιών AR και βραχιολιών. Τον Σεπτέμβριο του 2021, η εταιρεία ανακοίνωσε μια επένδυση 50 εκατομμυρίων δολαρίων σε παγκόσμιους εταίρους έρευνας και προγραμμάτων για να διασφαλίσει ότι η τεχνολογία metaverse θα αναπτυχθεί υπεύθυνα. [42]



Εικόνα 12: Ο διευθύνον σύμβουλος του Facebook δημιουργεί το δικό του avatar στο metaverse του Meta[42]

5.1. Κίνδυνοι

Μαζί με την έκρηξη του ενδιαφέροντος για το ψηφιακό νόμισμα και όλες τις επιπτώσεις του τόσο στις νέες όσο και στις παραδοσιακές επιχειρήσεις, υπάρχει μια αυξανόμενη ανάγκη για σαφήνεια σχετικά με τις νομικές επιπτώσεις αυτών των νέων τεχνολογιών και νομισμάτων. Καθώς οι κυβερνήσεις σε όλο τον κόσμο, οι ρυθμιστικοί φορείς, οι κεντρικές τράπεζες και άλλα χρηματοπιστωτικά ιδρύματα εργάζονται για να κατανοήσουν τη φύση και την έννοια των ψηφιακών νομισμάτων, οι μεμονωμένοι επενδυτές μπορούν να βγάλουν πολλά χρήματα επενδύοντας σε αυτόν τον νέο χώρο. Από την άλλη πλευρά, οι επενδυτές αναλαμβάνουν ορισμένους νομικούς κινδύνους όταν αγοράζουν και πωλούν κρυπτονομίσματα.

Ενώ το ψηφιακό χρήμα μπορεί είναι εύκολο να μπερδευτεί με το συμβατικό ηλεκτρονικό χρήμα, πρέπει να υπάρχει η γνώση πως δεν είναι το ίδιο. Το ίδιο ισχύει και για τα

κρυπτονομίσματα διότι δεν υπάρχει η αντίστοιχη φυσική του μορφή. Μεγάλο μέρος της ασάφειας για την νομική υπόσταση του ψηφιακού νομίσματος οφείλεται στο γεγονός ότι ο χώρος έγινε πρόσφατα δημοφιλής σε σύγκριση με τα πιο παραδοσιακά συστήματα νομισμάτων και πληρωμών. Παρακάτω, θα διερευνήσουμε ορισμένες από τις αναδυόμενες νομικές επιπτώσεις που σχετίζονται με την επένδυση σε κρυπτονομίσματα.

Οι επενδύσεις σε κρυπτονομίσματα έχουν γίνει διάχυτες και έχουν αναδείξει μια ποικιλία νομικών επιπτώσεων και κινδύνων που πρέπει να γνωρίζουν οι επενδυτές. Σε ορισμένες χώρες, το κρυπτονόμισμα θεωρείται νόμισμα, αλλά σε άλλες χώρες, όπως για παράδειγμα στις Ηνωμένες Πολιτείες, θεωρείται ιδιοκτησία και επομένως φορολογείται αναλόγως. Οι επενδυτές σε κρυπτονομίσματα πρέπει να πληρώνουν φόρους ανεξάρτητα από το που αγόρασαν το κρυπτονόμισμα. Το Bitcoin και διάφορα άλλα κρυπτονομίσματα είναι αποκεντρωμένα και ως εκ τούτου δεν υποστηρίζονται από καμία κεντρική αρχή, γεγονός που τα καθιστά ωφέλημα ή και επικίνδυνα για τους επενδυτές.

Οι επιχειρήσεις που δέχονται τα κρυπτονομίσματα δεν χρειάζεται μέχρι στιγμής να το καταγραφούν ή να έχουν κάποια άδεια, αλλά κάποια στιγμή μπορεί αυτό να αλλάξει και να χρειάζονται άδεια για να μπορούν να συνεχίσουν την λειτουργεία τους. Λόγω της αποκεντρωμένης φύσης της κρυπτογράφησης, ο κίνδυνος της εξαπάτησης αυξάνεται. Υπάρχει επίσης η πραγματικότητα ότι οι επενδυτές που έχουν υποστεί απάτη δεν θα έχουν την ίδια νομική προσφυγή με τα παραδοσιακά θύματα απάτης. [31]

5.1.1. Τα κρυπτονομίσματα ως ιδιοκτησία

Ένα από τα πιο κρίσιμα νομικά ζητήματα για κάθε επενδυτή κρυπτονομισμάτων έχει να κάνει με τον τρόπο με τον οποίο οι κεντρικές αρχές βλέπουν τα κρυπτονομίσματα. Στις ΗΠΑ για παράδειγμα, το IRS έχει ορίσει τα κρυπτονομίσματα ως ιδιοκτησία και όχι ως νόμισμα. Αυτό σημαίνει ότι οι επενδυτές υπόκεινται στους νόμους περί φορολογίας κεφαλαιουχικών κερδών όταν πρόκειται να αναφέρουν τα έξοδα και τα κέρδη τους περί κρυπτονομισμάτων στις ετήσιες φορολογικές τους δηλώσεις, ανεξάρτητα από το που τα αγόρασαν τα κρυπτονομίσματα.

Έτσι έχουν προστεθεί στον χώρο των κρυπτονομισμάτων επίπεδα σύγχυσης και πολυπλοκότητας για τους φορολογούμενους των ΗΠΑ. Ακόμα παραμένει ασαφές εάν οι επενδυτές ψηφιακών νομισμάτων που έχουν αγοράσει τις συμμετοχές τους σε από σελίδες του εξωτερικού, αν πρέπει να αντιμετωπίσουν πρόσθετα μέτρα υποβολής εκθέσεων όταν έρθει η ώρα της φορολογίας. Σύμφωνα με το CNBC, "όποιος έχει περισσότερα από 10.000 δολάρια στο εξωτερικό συνήθως χρειάζεται να συμπληρώνει την Έκθεση ξένων τραπεζών και χρηματοοικονομικών λογαριασμών (FBAR)... με το Υπουργείο Οικονομικών κάθε χρόνο ή το FATCA (απαιτεί από ορισμένους φορολογούμενους των ΗΠΑ να περιγράψουν τους λογαριασμούς τους από το εξωτερικό στο Έντυπο 8938, όταν υποβάλλουν τους φόρους τους στο IRS)."

Ο Kevin F. Sweeney -πρώην ομοσπονδιακός φορολογικός εισαγγελέας- έδωσε μια υπόδειξη σχετικά με το πώς οι ξένες ανταλλαγές κρυπτονομισμάτων θα μπορούσαν να περιπλέξουν τα φορολογικά ζητήματα για τους επενδυτές ψηφιακών νομισμάτων των ΗΠΑ: "πιθανώς υπάρχει μια απαίτηση του FBAR, αλλά δεν θα έφτανα τόσο μακριά ώστε να πω ότι υπάρχει πάντα", εξήγησε, προσθέτοντας ότι η έλλειψη καθοδήγησης από το IRS έχει δημιουργήσει μια αβεβαιότητα τόσο για τους επενδυτές όσο και για τους φορολογικούς επαγγελματίες. " Θα φαινόταν τρομερά άδικο αν περίμεναν από τους φορολογούμενους να το γνωρίζουν αυτό - και στη συνέχεια να επιβάλλουν κυρώσεις για τους φορολογούμενους που δεν το έκαναν - όταν οι επαγγελματίες δεν μπορούν καν να καταλάβουν 100% αν υπάρχει η απαίτηση από το FBAR", πρόσθεσε ο Sweeney κατά τη διάρκεια της συνέντευξη του στο CNBC.

Όλα αυτά υποδηλώνουν ότι οι επενδυτές ψηφιακών νομισμάτων θα πρέπει να λαμβάνουν ιδιαίτερες προφυλάξεις όσον αφορά την αναφορά κερδών και ζημιών σε κρυπτονομίσματα. Επειδή οι κανόνες αλλάζουν συνεχώς, αυτό που μπορεί να ήταν νομικά επιτρεπτό πέρυσι ή ακόμη και πριν από μήνες, όμως τώρα μπορεί να προκαλεί νομική ανησυχία. [31]

5.1.2. Η κατάσταση της αποκέντρωσης

Ένα από τα μεγάλα κέρδη πολλών ψηφιακών νομισμάτων είναι επίσης ο πιθανός παράγοντας κινδύνου για τον μεμονωμένο επενδυτή. Το Bitcoin (BTC) έχει ανοίξει το δρόμο για άλλα κρυπτονομίσματα, καθώς είναι αποκεντρωμένο, που σημαίνει ότι δεν έχει φυσική παρουσία και δεν υποστηρίζεται από καμία κεντρική αρχή. Ενώ οι κυβερνήσεις σε όλο τον κόσμο έχουν παρέμβει για να διεκδικήσουν τη ρυθμιστική του ισχύ με διάφορους τρόπους, το BTC και άλλα ψηφιακά νομίσματα όπως αυτό παραμένουν αποκεντρωμένα.

Από τη μία πλευρά, αυτό απαλλάσσει τους επενδυτές από το να είναι υπόχρεοι σε τέτοια ιδρύματα. Από την άλλη πλευρά, ωστόσο, αυτό το καθεστώς μπορεί να οδηγήσει σε νομικές επιπλοκές. Η αξία των ψηφιακών νομισμάτων εξαρτάται εξ ολοκλήρου από την αξία που τους αποδίδουν άλλοι ιδιοκτήτες και επενδυτές. Αυτό ισχύει για όλα τα νομίσματα, ψηφιακά ή ρευστά. Οι επενδυτές μπορεί να "μείνουν σε χλωρό κλαρί" αν προκύψουν επιπλοκές με τις συναλλαγές, χωρίς κάποια κεντρική αρχή που να μπορεί να τα ρυθμίζει.

Ένας άλλος πιθανός κίνδυνος που σχετίζεται με τα κρυπτονομίσματα έχει να κάνει με τα στοιχεία των συναλλαγών. Στις περισσότερες συναλλαγές, το νόμισμα που είναι φυσικό, αλλάζει χέρια. Στην περίπτωση του ηλεκτρονικού χρήματος, ένα αξιόπιστο χρηματοπιστωτικό ίδρυμα εμπλέκεται στη δημιουργία και τον διακανονισμό καταθέσεων και απαιτήσεων χρεών. Καμία από αυτές τις έννοιες δεν ισχύει για τις συναλλαγές κρυπτονομισμάτων. Εξαιτίας αυτής της διαφοράς, υπάρχει μια νομική σύγχυση μεταξύ των μερών σε διάφορους τύπους συναλλαγών ψηφιακών νομισμάτων. Λόγω της αποκεντρωμένης κατάστασης αυτών των νομισμάτων, η πορεία της νομικής προσφυγής σε αυτές τις καταστάσεις μπορεί να είναι δύσκολο να αξιολογηθεί. [31]

5.1.3. Επιχειρήσεις και αδειοδότηση

Ένας αυξανόμενος αριθμός επιχειρήσεων εκμεταλλεύεται τα ψηφιακά νομίσματα ως τον τρόπο πληρωμής. Όπως και σε άλλους χρηματοοικονομικούς τομείς, οι επιχειρήσεις μπορεί τελικά να υποχρεωθούν να εγγραφούν και να λάβουν άδεια για συγκεκριμένες δικαιοδοσίες και δραστηριότητες. Ωστόσο, λόγω του περίπλοκου και εξελισσόμενου νομικού καθεστώτος των ψηφιακών νομισμάτων, αυτός ο τομέας είναι πολύ λιγότερο σαφής για τις επιχειρήσεις που δραστηριοποιούνται στην αγορά κρυπτογράφησης.

Οι εταιρείες που δέχονται μόνο κρυπτονομίσματα, για παράδειγμα, μπορεί να μην χρειάζεται καθόλου να εγγραφούν ή/και να αποκτήσουν άδειες. Από την άλλη πλευρά, ενδέχεται να τους ζητηθεί να υποβληθούν σε ειδικές εκτιμήσεις ανάλογα με τη δικαιοδοσία τους. Το βάρος της ευθύνης βαρύνει τους ιδιοκτήτες και τους διευθυντές επιχειρήσεων να διασφαλίσουν ότι ακολουθούν τις κατάλληλες νομικές διαδικασίες για τις δραστηριότητές τους τόσο σε τοπικό όσο και σε κρατικό επίπεδο.

Για παράδειγμα, σε ομοσπονδιακό επίπεδο, τα χρηματοπιστωτικά ιδρύματα πρέπει να διατηρούν ορισμένες δραστηριότητες προστασίας από το ξέπλυμα χρήματος και την απάτη, τη διαβίβαση κεφαλαίων και άλλα. Σκέψεις σαν κι αυτές ισχύουν και για επιχειρήσεις που ασχολούνται με ψηφιακά νομίσματα. [31]

5.3.4. Ξέπλυμα χρήματος

Υπάρχει ευρέως μια διαδεδομένη πεποίθηση ότι τα κρυπτονομίσματα παρέχουν στις εγκληματικές οργανώσεις ένα μέσο για τη διάπραξη απάτης, νομιμοποίησης εσόδων από παράνομες δραστηριότητες και πλήθους άλλων οικονομικών εγκλημάτων. Αυτό μπορεί να μην επηρεάσει άμεσα τους περισσότερους επενδυτές κρυπτονομισμάτων που δεν σκοπεύουν να χρησιμοποιήσουν αυτή τη νέα τεχνολογία για να διαπράξουν εγκλήματα. Ωστόσο, οι επενδυτές που βρίσκονται στην ατυχή θέση να είναι θύματα οικονομικού εγκλήματος δεν έχουν πιθανώς τις ίδιες νομικές επιλογές με τα παραδοσιακά θύματα απάτης.

Αυτό το ζήτημα σχετίζεται επίσης και με την αποκεντρωμένη κατάσταση των ψηφιακών νομισμάτων. Για παράδειγμα, όταν ένα ανταλλακτήριο κρυπτονομισμάτων παραβιάζεται και κλαπούν τα στοιχεία των πελατών, δεν γίνεται να ανακτηθούν τα κεφάλαια. Έτσι, οι επενδυτές ψηφιακών νομισμάτων πρέπει να αναλαμβάνουν ένα συγκεκριμένο ποσό κινδύνου αγοράζοντας και διατηρώντας περιουσιακά στοιχεία κρυπτονομισμάτων.

Για αυτόν τον λόγο, οι προγραμματιστές και οι νεοσύστατες επιχειρήσεις που σχετίζονται με το ψηφιακό νόμισμα έχουν εστιάσει πολύ μεγάλη προσοχή στη δημιουργία ασφαλών μέσων για τη διατήρηση ψηφιακών νομισμάτων και των token. Παρότι, νέοι τύποι πορτοφολιών κυκλοφορούν συνεχώς και ενώ τα ανταλλακτήρια κρυπτονομισμάτων βελτιώνουν πάντα τα μέτρα ασφαλείας τους, οι επενδυτές δεν μπορούν να εξαλείψουν πλήρως τους νομικούς κινδύνους που σχετίζονται με την κατοχή κρυπτονομισμάτων και το πιθανότερο είναι ότι δεν θα μπορέσουν να το κάνουν ποτέ. [31]

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τα παραπάνω, μπορούμε να συμπεράνουμε ότι τα κρυπτονομίσματα δεν είναι μια ασφαλής επένδυση αλλά αντιθέτως υπάρχει μεγάλο ρίσκο, αλλά δεδομένου του ότι είναι κάτι πολύ καινούργιο, κανένας δεν ξέρει με σιγουριά που και πως θα πως θα εξελιχθεί. Οι τράπεζες παγκοσμίως θέλουν να υπάρξει μια τάξη(και όχι ένα χάος όπως αυτήν την στιγμή) στα κρυπτονομίσματα αλλά δεδομένου ότι από την φύση τους είναι αποκεντρωμένα, θα πρέπει να υπάρξουν νομοθεσίες σε κάθε χώρα για αυτά.

Από τεχνολογικής άποψης, το blockchain θεωρείτε το μέλλον του διαδικτύου και των χρηματοοικονομικών θεμάτων καθώς όλα είναι θεωρητικά πιο οργανωμένα από ότι είναι στην σήμερον ημέρα. Αντί να υπάρχει στην κάθε τράπεζα ξεχωριστά μια βάση δεδομένων, οποιοσδήποτε μπορεί να κατεβάσει μια βάση δεδομένων και να παρακολουθήσει τις συναλλαγές που έχουν πραγματοποιηθεί σε ένα συγκεκριμένο χρονικό διάστημα.

Βέβαια εκτός από τα θετικά του, υπάρχουν και σημαντικά αρνητικά τα οποία δεν έχουν λυθεί ακόμα. Το θέμα της ασφάλειας που παρέχεται από μια εταιρεία όπως η PayPal δεν μπορεί να εφαρμοστεί και στα κρυπτονομίσματα διότι δεν υπάρχει μια κεντρική αρχή που τα επιβλέπει. Εάν κλαπούν κρυπτονομίσματα από κάποιον τυχαίο επενδυτή, η αστυνομία δεν θα μπορεί να του προσφέρει την βοήθειά της διότι ο εγκληματίας, θα μπορούσε να είναι οποιοσδήποτε.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Icaew.com “History of blockchain” Published 2022. Accessed January 29, 2022. https://www.icaew.com/technical/technology/blockchain-and-cryptocurrency/blockchain-articles/what-is-blockchain/history.

[2] Wikipedia “Blockchain” Published January 28, 2022. Accessed January 29, 2022. https://en.wikipedia.org/wiki/Blockchain.

[3] Gichigi, T., & Gichigi, T. (2018, September 21). “A brief history of blockchain”. https://medium.com/coinmonks/a-brief-history-of-blockchain-70c519d3053.

[4] Binance Academy “The History of Blockchain Explained For Beginners” YouTube. Published online October 30, 2018. Accessed January 29, 2022. https://www.youtube.com/watch?v=ZbHLNinXy9E.

[5] Investopedia “Block (Bitcoin Block)” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/b/block-bitcoin-block.asp

[6] IG. “What is cryptocurrency trading and how does it work” Published 2019. Accessed January 29, 2022. https://www.ig.com/en/cryptocurrency-trading/what-is-cryptocurrency-trading-how-does-it-work.

[7] Yahoo.com “Crypto vs. Stocks: Which Is Better” Published 2018. Accessed January 29, 2022. https://finance.yahoo.com/news/crypto-vs-stocks-better-201720889.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHhrDsoLQKU3CUdU5CFnKTN5BLcUOmeo2OoWOoC9zBcRmpkDNkpWbW7IRdLaxSYINPsh1f5Ng4-Y2n7p_e5fD3oy7qVQPca0OK6XApdS0gh0bcYyr7DeZnPJJgbXvu9DRBSxf2ej3l5ZfmNSodyrg5woQWRvKUkrpS6UzSXGEZpy&guccounter=2.

[8] Yahoo.com “Top 10 DeFi Projects To Watch in 2022” Published 2022. Accessed January 29, 2022. https://finance.yahoo.com/news/top-10-defi-projects-watch-151711072.html.

[9] Investopedia “Bitcoin Definition: How Does Bitcoin Work” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/b/bitcoin.asp.

[10] Investopedia “What is a Cryptocurrency Public Ledger” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/.

[11] Wikipedia “Ethereum” Published January 28, 2022. Accessed January 29, 2022. https://en.wikipedia.org/wiki/Ethereum.

[12] Investopedia “Hard Fork (Blockchain) Definition” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/h/hard-fork.asp.

[13] Investopedia “Non-Fungible Token (NFT)” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/non-fungible-tokens-nft-5115211.

[14] Wikipedia “Non-fungible token” Published January 28, 2022. Accessed January 29, 2022. https://en.wikipedia.org/wiki/Non-fungible_token.

[15] Investopedia “Proof of Work (PoW)” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/p/proof-work.asp.

[16] Investopedia “Proof of Stake Definition” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/p/proof-stake-pos.asp.

[17] Gitbook.io “Proof of History - consensus” Published 2022. Accessed January 29, 2022. https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-history.

[18] Investopedia “What Is Proof of Burn for Cryptocurrency” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp.

[19] Investopedia “Mobile Wallet” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/m/mobile-wallet.asp.

[20] Investopedia “What Is a Digital Wallet” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/d/digital-wallet.asp.

[21] Wikipedia “Digital wallet” Published January 18, 2022. Accessed January 29, 2022. https://en.wikipedia.org/wiki/Digital_wallet.

[22] SearchCIO “Baker P. Today’s blockchain use cases and industry applications” Published 2017. Accessed January 29, 2022. https://www.techtarget.com/searchcio/feature/Todays-blockchain-use-cases-and-industry-applications.

[23] The European Business Review. “Editor EBR. The European Business Review” Published November 2021. Accessed January 29, 2022. https://www.europeanbusinessreview.com/future-of-blockchain-how-will-it-revolutionize-the-world-in-2022-beyond/.

[24] Hackernoon.com “Beyers J. Blockchain Beyond Fintech” Published May 16, 2018. Accessed January 29, 2022. https://hackernoon.com/blockchain-beyond-fintech-dff940d072fe.

[25] Vxchnge.com. “Seal A. Centralized vs Decentralized Network: Which One Do You Need” Published 2020. Accessed January 29, 2022. https://www.vxchnge.com/blog/centralized-decentralized-network.

[26] Investopedia. “Decentralized Market Definition” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/d/decentralizedmarket.asp.

[27] @coindesk Hertig A. “What Is DeFi” Published September 18, 2020. Accessed January 29, 2022. https://www.coindesk.com/learn/what-is-defi/.

[28] Choudhury N. *World Wide Web and Its Journey from Web 1.0 to Web 4.0*. https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf

[29] Investopedia “Decentralized Autonomous Organization (DAO)” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/tech/what-dao/.

[30]Investopedia “What Is Stablecoin” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/s/stablecoin.asp.

[31]Investopedia “What Are the Legal Risks to Cryptocurrency Investors” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/tech/what-are-legal-risks-cryptocurrency-investors/.

[32]Investopedia “Blockchain Explained” Published 2022. Accessed January 29, 2022. https://www.investopedia.com/terms/b/blockchain.asp.

[33] Top 5 Cryptocurrency to Invest in 2022. Money Excel - Personal Finance Blog. Published April 4, 2021. Accessed April 3, 2022. https://moneyexcel.com/top-5-cryptocurrency-to-invest-in-2021/

[34] Springer Verlag. An example of a smart contract written in Solidity. ResearchGate. Published May 2020. Accessed April 3, 2022. https://www.researchgate.net/figure/An-example-of-a-smart-contract-written-in-Solidity_fig1_337603517

[35] Vitalik Buterin has earned $4.3 million from his $25.000 investment in Dogecoin ... so far - Digital Currencies. Digital Currencies. Published June 12, 2021. Accessed April 3, 2022. https://digitalcurrencies.page/vitalik-buterin-has-earned-4-3-million-from-his-25-000-investment-in-dogecoin-so-far/

[36] Sharma S. Is CryptoKitties the Next Breakout NFT Collectible? Trading Volume Data Indicates so. CoinGape. Published September 3, 2021. Accessed April 3, 2022. https://coingape.com/is-cryptokitties-the-next-breakout-nft-collectible-trading-volume-data-indicates-so/

[37] Stablecoins | ethereum.org. Published 2022. Accessed April 3, 2022. https://ethereum.org/en/stablecoins/

[38] Fig. 7. Proof of Work Flowchart. ResearchGate. Published December 2018. Accessed April 3, 2022. https://www.researchgate.net/figure/Proof-of-Work-Flowchart_fig6_331040157

[39] Figure 3. Proof-of-Stake flow. ResearchGate. Published August 22, 2019. Accessed April 3, 2022. https://www.researchgate.net/figure/Proof-of-Stake-flow_fig3_335337656

[40] Hot wallet vs. Cold wallet | Bitcoin business, Blockchain cryptocurrency, Cryptocurrency trading. Pinterest. Published 2022. Accessed April 3, 2022. https://www.pinterest.com/pin/725924033667320642/

[41]Comparison of Web 1.0, Web 2.0 and Web 3.0. ResearchGate. Published March 2015. Accessed April 3, 2022. https://www.researchgate.net/figure/Comparison-of-Web-10-Web-20-and-Web-30_tbl1_280944777

[42] Wilson G. Facebook Connect LIVE: Zuckerberg’s company gives more details of its metaverse. 24 News Recorder. Published October 28, 2021. Accessed April 3, 2022. https://24newsrecorder.com/technology/47132

[43] How Does Bitcoin Mining Work? Investopedia. Published 2022. Accessed May 30, 2022. https://www.investopedia.com/tech/how-does-bitcoin-mining-work