University of Macedonia
MSc in Applied Informatics

Ψηφιακά Νομίσματα

&

Blockchain Τεχνολογία

ΠΕΡΙΛΗΨΗ

Το πρώτο ψηφιακό νόμισμα που έθεσε τα θεμέλια για την επανάσταση στο παγκόσμιο χρηματοπιστωτικό σύστημα, ήταν το Bitcoin, το οποίο εισήχθη το 2009, προσφέροντας μια αποκεντρωμένη εναλλακτική λύση στις παραδοσιακές τραπεζικές διαδικασίες. Αν και δεν αναγνωρίζεται επίσημα ως νόμιμο χρήμα, η δημοτικότητα και η χρήση του, όπως και άλλων κρυπτονομισμάτων, έχουν αυξηθεί δραματικά τα τελευταία χρόνια. Αυτή η αύξηση συνδέεται άμεσα με τις τεράστιες διακυμάνσεις στις τιμές τους, οι οποίες αντικατοπτρίζουν τη ρευστότητα και την υψηλή μεταβλητότητα αυτών των αγορών, καθιστώντας τα ταυτόχρονα ελκυστικά και ριψοκίνδυνα επενδυτικά μέσα. Στη βάση αυτής της επανάστασης βρίσκεται η τεχνολογία Blockchain, που όχι μόνο υποστηρίζει το Bitcoin αλλά έχει προσελκύσει μεγάλο ενδιαφέρον για τις εφαρμογές της σε διάφορους τομείς πέρα από τα κρυπτονομίσματα, όπως οι χρηματοοικονομικές υπηρεσίες, η διαχείριση εφοδιαστικής αλυσίδας, κ.α., παρέχοντας τη δυνατότητα για ασφαλέστερες, πιο διαφανείς και αποκεντρωμένες συναλλαγές. Ωστόσο, παρά τα οφέλη που προσφέρουν τα ψηφιακά νομίσματα, υπάρχουν σοβαρές προκλήσεις που πρέπει να αντιμετωπιστούν, όπως είναι η επεκτασιμότητα των δικτύων, η αυξημένη κατανάλωση ενέργειας, καθώς και οι ανησυχίες για την ασφάλεια και την ιδιωτικότητα των συναλλαγών. Επιπλέον, η κεφαλαιοποίηση της αγοράς των κρυπτονομισμάτων είναι κρίσιμος παράγοντας για την εκτίμηση της αξίας και του κινδύνου που αυτά ενέχουν.

Καταλήγοντας, το μέλλον τους φαίνεται υποσχόμενο, αλλά παραμένει αβέβαιο. Οι τιμές τους θα συνεχίσουν να υπόκεινται σε διακυμάνσεις, επηρεαζόμενες από τη ζήτηση, τις ρυθμιστικές πολιτικές, και τις τεχνολογικές εξελίξεις. Ειδικότερα, σύμφωνα με ορισμένες προβλέψεις, το Bitcoin ενδέχεται να φτάσει σε νέες ιστορικές τιμές το 2025, καθώς η αυξανόμενη υιοθέτηση και αναγνώρισή του από επενδυτές και επιχειρήσεις δημιουργεί ευνοϊκές συνθήκες για την άνοδο της αξίας του. Ωστόσο, η μακροπρόθεσμη επιτυχία των κρυπτονομισμάτων θα εξαρτηθεί από το κατά πόσο η αγορά θα καταφέρει να ξεπεράσει τις υπάρχουσες προκλήσεις και να εδραιώσει ένα σταθερό και αποτελεσματικό ρυθμιστικό πλαίσιο που θα εγγυάται τη βιωσιμότητά τους στο μέλλον.

Λέξεις-κλειδιά: ψηφιακά νομίσματα, bitcoin, κρυπτονομίσματα, blockchain τεχνολογία, αποκέντρωση

ABSTRACT

The first digital currency that laid the foundation for the revolution in the global financial system was Bitcoin, introduced in 2009. It offered a decentralized alternative to traditional banking processes. Although it is not officially recognized as legal tender, the popularity and use of Bitcoin, along with other cryptocurrencies, have increased dramatically in recent years. This growth is directly linked to the massive price fluctuations of cryptocurrencies, which reflect the liquidity and high volatility of these markets, making them both attractive and risky investments. At the core of this revolution is Blockchain technology, which not only supports Bitcoin but has also attracted significant interest for its applications in various sectors beyond cryptocurrencies, such as financial services, supply chain management, and more. Blockchain provides the potential for safer, more transparent, and decentralized transactions. However, despite the benefits offered by digital currencies, there are serious challenges that must be addressed, including network scalability, increased energy consumption, and concerns about transaction security and privacy. Additionally, the market capitalization of cryptocurrencies is a critical factor in assessing their value and the risk they entail.

In conclusion, the future of digital currencies appears promising, but it remains uncertain. Their prices will continue to fluctuate, influenced by demand, regulatory policies, and technological developments. Specifically, according to some predictions, Bitcoin may reach new all-time highs by 2025, as its adoption and recognition by investors and businesses are expected to increase, creating favorable conditions for its value to rise. However, the long-term success of cryptocurrencies will depend on whether the market can overcome existing challenges and establish a stable and effective regulatory framework that ensures their sustainability in the future.

Keywords: digital currencies, bitcoin, cryptocurrencies, blockchain technology, decentralization

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 2
ABSTRACT 3
ΕΙΣΑΓΩΓΗ 5
ΚΕΦΑΛΑΙΟ 1. ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ 7
1.1 Εισαγωγή στα Ψηφιακά Νομίσματα 7
1.2. Bitcoin – Το Πρώτο Ψηφιακό Νόμισμα 9
1.2.1. Η Γέννηση του Bitcoin 9
1.2.2. Παράγοντες που επηρεάζουν το Bitcoin 11
1.3. Η Εξέλιξη των Ψηφιακών Νομισμάτων 13
1.3.1. Κατηγορίες των Ψηφιακών Νομισμάτων 13
1.3.2. Η Άνοδος των ICOs και η Ρυθμιστική Αντίδραση 16
1.3.3. Εισαγωγή των Κεντρικών Τραπεζών στα Ψηφιακά Νομίσματα 17
1.4. Τεχνολογικές Προκλήσεις 19
1.5. Επιδράσεις των Ψηφιακών Νομισμάτων στην Παγκόσμια Οικονομία 22
ΚΕΦΑΛΑΙΟ 2. ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN 27
2.1. Ορισμός και Κύρια Χαρακτηριστικά 27
2.1.1. Οι Τύποι Blockchain 29
2.1.2. Μηχανισμοί Συναίνεσης 34
2.2. Δομή και Λειτουργία 41
2.3. Εφαρμογές της Τεχνολογίας Blockchain 46
2.4. Προκλήσεις και Περιορισμοί της Τεχνολογίας Blockchain 49
2.5. Το Μέλλον της Τεχνολογίας Blockchain 51
ΚΕΦΑΛΑΙΟ 3. ΟΙΚΟΝΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΤΩΝ ΨΗΦΙΑΚΩΝ ΝΟΜΙΣΜΑΤΩΝ 53
3.1. Τρέχον Μερίδιο Αγοράς 53
3.1.1. Κεφαλαιοποίηση της Αγοράς των Ψηφιακών Νομισμάτων 53
3.1.2. Τρέχον Μερίδιο Αγοράς των Ψηφιακών Νομισμάτων 56
3.2. Παράγοντες που επηρεάζουν το Μερίδιο Αγοράς των Ψηφιακών Νομισμάτων 60
3.3. Επενδυτικές Στρατηγικές των Ψηφιακών Νομισμάτων 64
3.4. Μελλοντικό Μερίδιο Αγοράς 70
ΣΥΜΠΕΡΑΣΜΑΤΑ 73
ΜΕΘΟΔΟΛΟΓΙΑ PRISMA 74
ΒΙΒΛΙΟΓΡΑΦΙΑ 77

ΕΙΣΑΓΩΓΗ

Η εξέλιξη της τεχνολογίας έχει επιφέρει ριζικές αλλαγές σε όλους τους τομείς της κοινωνίας και της οικονομίας, με τα ψηφιακά νομίσματα να αποτελούν μια από τις πιο καινοτόμες και επίκαιρες εξελίξεις στον χρηματοοικονομικό τομέα. Τα ψηφιακά νομίσματα, τα οποία βασίζονται σε πρωτοποριακές τεχνολογίες, όπως το blockchain, έχουν αρχίσει να αμφισβητούν την κυριαρχία των παραδοσιακών μορφών χρήματος, προκαλώντας ταυτόχρονα έντονες συζητήσεις σχετικά με το μέλλον της οικονομίας και των χρηματοπιστωτικών συστημάτων. Η εμφάνιση του Bitcoin το 2009, ως το πρώτο ψηφιακό νόμισμα, αποτέλεσε σημείο καμπής στην ιστορία των οικονομικών συναλλαγών, εισάγοντας μια νέα μορφή χρήματος που βασίζεται στην αποκέντρωση και στην ασφάλεια μέσω της κρυπτογραφίας.

Το Bitcoin δεν είναι απλώς ένα νέο μέσο ανταλλαγής αξίας, αλλά αντιπροσωπεύει μια επαναστατική αλλαγή στον τρόπο με τον οποίο αντιλαμβανόμαστε και χρησιμοποιούμε το χρήμα. Η τεχνολογία blockchain, που υποστηρίζει τη λειτουργία του Bitcoin και άλλων κρυπτονομισμάτων, εισήγαγε έναν καινοτόμο τρόπο αποθήκευσης και διαχείρισης δεδομένων. Αυτή η τεχνολογία, με την αποκεντρωμένη και διαφανή φύση της, εξαλείφει την ανάγκη για ενδιάμεσους, όπως οι τράπεζες, και διασφαλίζει την ακεραιότητα των συναλλαγών μέσω ενός κατανεμημένου δικτύου υπολογιστών. Η εισαγωγή αυτής της τεχνολογίας δημιούργησε νέες προοπτικές και προκλήσεις, ενώ παράλληλα έθεσε τα θεμέλια για μια σειρά από καινοτομίες και εφαρμογές που ξεπερνούν τον χρηματοοικονομικό τομέα, επηρεάζοντας πολλούς άλλους κλάδους, όπως η εφοδιαστική αλυσίδα, η υγεία και η δημόσια διοίκηση.

Ο στόχος αυτής της εργασίας είναι να προσφέρει μια ολοκληρωμένη ανάλυση και κατανόηση των ψηφιακών νομισμάτων και της τεχνολογίας Blockchain, εστιάζοντας στην ιστορική τους εξέλιξη, την τρέχουσα κατάσταση και τον αντίκτυπό τους στην παγκόσμια οικονομία. Μέσα από την εξέταση των τεχνολογικών, οικονομικών και ρυθμιστικών παραμέτρων, η εργασία αποσκοπεί να αναδείξει τον ρόλο και την επιρροή των ψηφιακών νομισμάτων και της τεχνολογίας Blockchain, καθώς και να αξιολογήσει τις υπάρχουσες προβλέψεις για τις μελλοντικές τάσεις και προκλήσεις που ενδέχεται να προκύψουν από την ευρύτερη υιοθέτησή

τους. Επιπλέον, με τη χρήση της μεθοδολογίας PRISMA, εξασφαλίζεται η αναλυτική προσέγγιση της έρευνας, προσφέροντας πληρότητα και αξιοπιστία στη μελέτη.

Η εργασία είναι οργανωμένη σε τρία βασικά κεφάλαια:

Στο Κεφάλαιο 1, παρουσιάζεται μια εκτενής εισαγωγή στα ψηφιακά νομίσματα, με ιδιαίτερη έμφαση στο Bitcoin, το οποίο είναι το πρώτο και πιο γνωστό ψηφιακό νόμισμα. Αναλύεται η δημιουργία Bitcoin, οι παράγοντες που το επηρεάζουν, καθώς και η εξέλιξη των ψηφιακών νομισμάτων σε διάφορες κατηγορίες. Εξετάζεται επίσης η άνοδος των ICOs και η αντίδραση των ρυθμιστικών αρχών, καθώς και η εμπλοκή των κεντρικών τραπεζών. Τέλος, συζητούνται οι τεχνολογικές προκλήσεις και οι επιπτώσεις των ψηφιακών νομισμάτων στην παγκόσμια οικονομία.

Το Κεφάλαιο 2 εστιάζει στην τεχνολογία Blockchain, η οποία αποτελεί τη θεμέλια τεχνολογία των ψηφιακών νομισμάτων. Αρχικά, παρέχεται ένας ορισμός της τεχνολογίας και των κύριων χαρακτηριστικών της, ακολουθούμενος από την ανάλυση των διαφορετικών τύπων Blockchain και των μηχανισμών συναίνεσης που χρησιμοποιούνται. Στη συνέχεια, εξετάζεται η δομή και η λειτουργία του Blockchain, οι διάφορες εφαρμογές του, οι προκλήσεις και οι περιορισμοί του, καθώς και οι προοπτικές για το μέλλον της τεχνολογίας αυτής.

Το Κεφάλαιο 3 ασχολείται με τα οικονομικά στοιχεία των ψηφιακών νομισμάτων. Εξετάζεται το τρέχον μερίδιο αγοράς και η κεφαλαιοποίηση της αγοράς των ψηφιακών νομισμάτων, καθώς και οι παράγοντες που επηρεάζουν το μερίδιο αγοράς. Επιπλέον, αναλύονται οι επενδυτικές στρατηγικές που ακολουθούνται στον χώρο των ψηφιακών νομισμάτων και γίνονται προβλέψεις για το μελλοντικό μερίδιο αγοράς.

ΚΕΦΑΛΑΙΟ 1. ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ

1.1 Εισαγωγή στα Ψηφιακά Νομίσματα

Τα ψηφιακά νομίσματα αποτελούν μια μορφή νομίσματος που υπάρχει αποκλειστικά σε ψηφιακή ή ηλεκτρονική μορφή. Πιο συγκεκριμένα, το ψηφιακό νόμισμα είναι ένας όρος που αναφέρεται σε ηλεκτρονική αξία, η οποία δημιουργείται και κυκλοφορεί στο διαδίκτυο, χωρίς να χρειάζεται η μεσολάβηση των παραδοσιακών τραπεζών (Rose, C. (2015)). Επιπλέον, τα ψηφιακά νομίσματα διαθέτουν κάποια, αλλά όχι όλα τα χαρακτηριστικά ενός παραδοσιακού νομίσματος. Ενδέχεται επίσης να παρουσιάζουν χαρακτηριστικά ενός εμπορεύματος ή άλλου περιουσιακού στοιχείου. Παρά την αυξανόμενη δημοτικότητά τους, κανένα από αυτά τα ψηφιακά νομίσματα δεν έχει αναγνωριστεί επίσημα ως νόμιμο χρήμα σε καμία χώρα. Μοναδική εξαίρεση αποτελεί το Ελ Σαλβαδόρ, το οποίο το 2021 αναγνώρισε το Bitcoin ως επίσημο νόμισμά του.

Ειδικότερα, η έννοια των ψηφιακών νομισμάτων άρχισε να διαμορφώνεται τη δεκαετία του 1980, παράλληλα με την ανάπτυξη του διαδικτύου και των τεχνολογιών πληροφορίας. Μία από τις πρώτες προσπάθειες ψηφιακού νομίσματος για τη δημιουργία ανώνυμων και ασφαλών ηλεκτρονικών πληρωμών ήταν το DigiCash, που ιδρύθηκε το 1989 από τον Αμερικανό κρυπτογράφο David Chaum, ο οποίος θεωρείται ο "πατέρας των κρυπτονομισμάτων". Ήδη από το 1983, ο Chaum είχε δημοσιεύσει την ιδέα για το ανώνυμο ηλεκτρονικό χρήμα, που ονόμασε eCash. Παρόλο που η DigiCash υλοποίησε αυτήν την ιδέα μέσω μιας τράπεζας, δεν κατάφερε να αποκτήσει σημαντική αποδοχή από τους χρήστες, και τελικά η τράπεζα αποκτήθηκε από έναν μεγάλο εκδότη πιστωτικών καρτών, οδηγώντας στη διάλυση της το 1998. Παρόμοια, το e-Gold, μια πλατφόρμα που ιδρύθηκε το 1996 και επέτρεπε τη χρήση χρυσού ως ηλεκτρονικό χρήμα, αντιμετώπισε νομικά προβλήματα και έκλεισε. Ωστόσο, η πραγματική επανάσταση στον χώρο των ψηφιακών νομισμάτων ήρθε το 2009 με την εισαγωγή του Bitcoin, του πρώτου αποκεντρωμένου ψηφιακού νομίσματος, το οποίο βασίστηκε στην τεχνολογία Blockchain. Το Bitcoin άνοιξε τον δρόμο για την ανάπτυξη χιλιάδων άλλων κρυπτονομισμάτων και καθιέρωσε τα ψηφιακά νομίσματα ως μια σημαντική εναλλακτική μορφή πληρωμής και επένδυσης στην παγκόσμια οικονομία.

Η ιδέα για τα ψηφιακά νομίσματα βασίζεται στην έννοια ότι η ανταλλαγή αξίας δεν απαιτεί πλέον την ανταλλαγή φυσικών αντικειμένων. Από τότε που δημιουργήθηκε το εμπορικό Διαδίκτυο, μοναδικοί ψηφιακοί σειριακοί αριθμοί μπορούν να κυκλοφορούν με ασφάλεια στο διαδίκτυο, αντικαθιστώντας τα φυσικά αγαθά και διευκολύνοντας τις συναλλαγές με τρόπους που ήταν αδιανόητοι λίγες δεκαετίες πριν. Ειδικότερα, τα συστήματα ψηφιακού νομίσματος περιλαμβάνουν τη μεταφορά αξίας και τη διαχείριση των συναλλαγών μέσω διαδικτύου. Έτσι λοιπόν, ένα κλειστό σύστημα λογιστικής στο διαδίκτυο μπορεί εύκολα να προσαρμοστεί ώστε να λειτουργεί ως ψηφιακό νόμισμα (Mullan, P.C. (2014)). Επειδή αυτά τα συστήματα πληρωμών δεν βασίζονται στις παραδοσιακές τράπεζες, προσφέρουν νέες, πιο οικονομικές λύσεις για χρηματοοικονομικές υπηρεσίες σε όλο τον κόσμο.

Bitcoin	Ethereum	BNB	Solana	USD Coin
Bitcoin Cash	Ethereum Classic	Titcoin	VEN	IOTA
Dogecoin	Litecoin	Chinacoin	Steller Lumens	Mazacoin
Cardano	Dash	NXT	Zcash	EOS
Tether	Monero (XMR)	Primecoin	Namecoin	NEO
Toncoin	NEM	Auroracoin	Remnibi	Verge
Vertcoin	Nano	Gridcoin	XRP	TRON

Πίνακας 1. Παραδείγματα Ψηφιακών Νομισμάτων.

Αξίζει να σημειωθεί ότι, τα ψηφιακά νομίσματα διαφέρουν σημαντικά από τα παραδοσιακά νομίσματα. Καταρχάς, ενώ τα παραδοσιακά νομίσματα εκδίδονται από κυβερνήσεις και κεντρικές τράπεζες και υπάρχουν σε φυσική μορφή, όπως χαρτονομίσματα και κέρματα, τα ψηφιακά νομίσματα έχουν καθαρά ψηφιακή μορφή και δεν έχουν φυσική υπόσταση. Επιπλέον, υπάρχει διαφορά στον τρόπο με τον οποίο ελέγχονται. Συγκεκριμένα, ενώ τα παραδοσιακά ρυθμίζονται από κεντρικές τράπεζες, που καθορίζουν τη νομισματική πολιτική και ελέγχουν την ποσότητα του χρήματος που κυκλοφορεί στην αγορά, τα ψηφιακά μπορούν να λειτουργούν ανεξάρτητα από τέτοιες αρχές. Χαρακτηριστικό παράδειγμα είναι τα κρυπτονομίσματα, όπου η αξία τους και οι συναλλαγές καθορίζονται από τις δυνάμεις της προσφοράς και της ζήτησης στην αγορά. Τέλος, όσον αφορά τις συναλλαγές, τα παραδοσιακά νομίσματα επιτρέπουν τόσο τις φυσικές συναλλαγές, όπως η χρήση μετρητών, όσο και τις ηλεκτρονικές, μέσω καρτών και τραπεζικών μεταφορών. Αντίθετα, τα ψηφιακά νομίσματα βασίζονται σε τεχνολογίες όπως το blockchain για την καταγραφή των συναλλαγών, προσφέροντας μεγαλύτερη διαφάνεια και ασφάλεια στις συναλλαγές.

1.2. Bitcoin – Το Πρώτο Ψηφιακό Νόμισμα

1.2.1. Η Γέννηση του Bitcoin

Κατά τη διάρκεια της παγκόσμιας οικονομικής κρίσης του 2008, οι αδυναμίες του παραδοσιακού τραπεζικού συστήματος έγιναν εμφανείς, γεγονός που τόνισε την ανάγκη για νέες, εναλλακτικές μορφές οικονομικών συναλλαγών, ανεξάρτητες από κεντρικές αρχές ή κυβερνήσεις. Μέσα σε αυτό το κλίμα, γεννήθηκε η ιδέα για το Bitcoin (BTC), ως το αποτέλεσμα της σκέψης ενός ατόμου ή μιας ομάδας προγραμματιστών, που χρησιμοποίησε το ψευδώνυμο Satoshi Nakamoto. Αυτή η ιδέα ήταν η απάντηση στην κρίση εμπιστοσύνης προς τις τράπεζες και τα χρηματοοικονομικά συστήματα.

Η εμφάνισή του Bitcoin σηματοδότησε μια νέα εποχή στον τομέα των χρηματοοικονομικών συναλλαγών και της έννοιας του χρήματος. Συγκεκριμένα, είχε ως στόχο τη δημιουργία ενός αποκεντρωμένου ψηφιακού νομίσματος, απαλλαγμένου από τον έλεγχο κεντρικών αρχών, όπως οι κυβερνήσεις και οι τράπεζες. Αντίθετα, για να διασφαλιστεί η ασφάλεια και η ακρίβεια των συναλλαγών με Bitcoin, αυτές θα επαληθεύονταν και θα καταγράφονταν σε ένα δημόσιο λογιστικό βιβλίο, γνωστό ως blockchain, το οποίο αποτελεί ένα δίκτυο κόμβων που συνεργάζονται για να επιτύχουν αυτόν τον στόχο.

Πιο αναλυτικά όμως, όλα ξεκίνησαν στις 31 Οκτωβρίου 2008, όταν ο Satoshi Nakamoto δημοσίευσε το Λευκό Έγγραφο του Bitcoin, ένα κείμενο 8 σελίδων με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, S. (2008)). Το έγγραφο αυτό περιέγραφε λεπτομερώς την τεχνολογία πίσω από το Bitcoin και την ιδέα ενός αποκεντρωμένου ψηφιακού νομίσματος. Ο Nakamoto παρουσίασε ένα σύστημα ηλεκτρονικών συναλλαγών που βασίζεται στην κρυπτογραφία και επιτρέπει στους χρήστες να πραγματοποιούν συναλλαγές απευθείας μεταξύ τους, χωρίς την ανάγκη για διαμεσολαβητές όπως τράπεζες ή χρηματοπιστωτικά ιδρύματα. Σύμφωνα με το Λευκό Έγγραφο, μια από τις κύριες καινοτομίες του Bitcoin ήταν η χρήση του blockchain, ενός κατανεμημένου δικτύου υπολογιστών για την επαλήθευση των συναλλαγών. Το σύστημα αυτό όχι μόνο εξασφάλιζε την ασφάλεια των συναλλαγών μέσω της κρυπτογραφίας αλλά μπορούσε να αντιμετωπίσει το πρόβλημα της διπλής δαπάνης (double-spending), το οποίο αποτελούσε μια σημαντική πρόκληση για τα ψηφιακά νομίσματα πριν από

την εμφάνιση του Bitcoin. Με τον όρο αυτό, αναφερόμαστε στην περίπτωση όπου ένας χρήστης μπορεί να προσπαθήσει να ξοδέψει το ίδιο ψηφιακό νόμισμα περισσότερες από μία φορές, κάτι που θα υπονόμευε την αξιοπιστία του συστήματος. Επιπλέον, το έγγραφο εισήγαγε την έννοια του "proof-of-work" μια διαδικασία που χρησιμοποιείται για την εξόρυξη νέων bitcoins και την ενίσχυση της ασφάλειας του δικτύου.

Στις 3 Ιανουαρίου 2009, ο Satoshi προχώρησε από τη θεωρία στην πράξη, δημιουργώντας το πρώτο block, γνωστό και ως "Genesis Block" ή Block 0, το οποίο περιείχε τα πρώτα 50 Bitcoins. Μέσα στον κώδικα αυτού του block συμπεριέλαβε ένα μήνυμα: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.", αναφερόμενος στο πρωτοσέλιδο της βρετανικής εφημερίδας The Times, που έγραφε για την ανάγκη ενός δεύτερου πακέτου διάσωσης των τραπεζών. Εκείνη την εποχή, οι κυβερνήσεις αναγκάστηκαν να δαπανήσουν τεράστια ποσά δισεκατομμυρίων για να αποτρέψουν την κατάρρευση του τραπεζικού συστήματος.

Λίγο αργότερα, στις 12 Ιανουαρίου 2009, ο Satoshi Nakamoto πραγματοποίησε την πρώτη συναλλαγή με Bitcoin, στέλνοντας τα πρώτα 10 bitcoins στον προγραμματιστή και κρυπτογράφο Hal Finney. Ο Finney, ένας από τους πρώτους που ασχολήθηκαν ενεργά με το Bitcoin, έπαιξε καθοριστικό ρόλο στην αρχική του ανάπτυξη. Αυτή η συναλλαγή, η πρώτη που καταγράφηκε στο δίκτυο, σηματοδότησε την έναρξη της λειτουργίας του Bitcoin ως ψηφιακού νομίσματος και θεωρείται η πρώτη επίσημη μεταφορά bitcoin.

Όσον αφορά την αποδοχή του, στην αρχή το Bitcoin έγινε αποδεκτό μόνο από μια μικρή κοινότητα τεχνολογικών ενθουσιωδών και κρυπτογράφων, καθώς οι περισσότεροι από τους πρώτους χρήστες του ήταν άτομα με τεχνικές γνώσεις ή ενδιαφέρον για την καινοτόμο τεχνολογία Blockchain. Παρά την αρχική επιφύλαξη που υπήρχε γύρω από αυτό, σταδιακά άρχισε να αποκτά όλο και περισσότερους υποστηρικτές και να αναγνωρίζεται ως ένα καινοτόμο εργαλείο στον χώρο των ψηφιακών πληρωμών και της οικονομικής ανεξαρτησίας. Με την πάροδο του χρόνου, η αποδοχή του Bitcoin επεκτάθηκε σε ένα ευρύτερο κοινό, καθώς όλο και περισσότεροι άνθρωποι διέκριναν τις προοπτικές του ως εναλλακτικό σύστημα χρημάτων και επενδύσεων. Σήμερα, το Bitcoin έχει κατακτήσει την παγκόσμια αναγνώριση και γίνεται αποδεκτό από χιλιάδες επιχειρήσεις και οργανισμούς, καθιερώνοντάς το ως το πιο γνωστό και πρωτοποριακό κρυπτονόμισμα.

Με την εδραίωση του Bitcoin και την αυξανόμενη αποδοχή του, ο Satoshi Nakamoto, το 2010, αποφάσισε να αποσυρθεί από την ενεργή συμμετοχή στην ανάπτυξή του. Παραχώρησε τον έλεγχο του αποθετηρίου κώδικα και των σχετικών δικτύων σε άλλα μέλη της κοινότητας, αφήνοντας πίσω του ένα μυστήριο, καθώς η πραγματική του ταυτότητα παραμένει άγνωστη μέχρι και σήμερα.

1.2.2. Παράγοντες που επηρεάζουν το Bitcoin

Είναι πολύ σημαντικό να εξετάσουμε τους παράγοντες που επηρέασαν τις πρώτες συναλλαγές και την αρχική διαμόρφωση των τιμών του Bitcoin, ώστε να κατανοήσουμε την μετέπειτα εξέλιξή του. Ξεκινώντας λοιπόν, το 2009, το Bitcoin ήταν ένα πολύ εξειδικευμένο και χαμηλής ρευστότητας περιουσιακό στοιχείο. Ειδικότερα, οι συναλλαγές γίνονταν κυρίως εκτός οργανωμένων αγορών (Over-The-Counter (OTC)), μέσω φόρουμ όπως το BitcoinTalk, από χρήστες που αναγνώριζαν την αξία του ως αποκεντρωμένο νόμισμα. Ένα χαρακτηριστικό παράδειγμα, αποτέλεσε η πρώτη εμπορική χρήση του στις 22 Μαΐου 2010, όταν ο προγραμματιστής Laszlo Hanyecz προσέφερε 10.000 BTC σε έναν χρήστη του BitcoinTalk, ο οποίος παρήγγειλε δύο πίτσες για αυτόν. Εκείνη την περίοδο, το Bitcoin είχε ακόμα πολύ χαμηλή αξία, κάτω από 0.01 δολάρια, και οι χρήστες του BitcoinTalk θεώρησαν αυτή τη συναλλαγή ως μια πρωτοποριακή κίνηση, σε αντίθεση με τη σημερινή χρήση του για την αγορά καθημερινών αγαθών μέσω καρτών όπως η Binance Visa.
Ωστόσο, με την άνοδο της τιμής και της δημοτικότητας του, άρχισε να αναπτύσσεται μια μικρή, ανεξέλεγκτη βιομηχανία που διευκόλυνε τις συναλλαγές και τις αγοραπωλησίες του. Η βιομηχανία αυτή περιελάμβανε πλατφόρμες ανταλλαγής κρυπτονομισμάτων και αγορές στο deep web (τμήμα του διαδικτύου που δεν είναι προσβάσιμο μέσω συμβατικών μηχανών αναζήτησης). Επειδή όμως, η πορεία αυτών των αγορών/ανταλλακτηρίων δεν ήταν σταθερή, εξαιτίας παραβιάσεων, κλεισίματος ή άλλων ρυθμίσεων τους, η τιμή του Bitcoin, υπέστη πολλές διακυμάνσεις. Επιπλέον, πολλά από αυτά κατείχαν μεγάλες ποσότητες Bitcoin, προκαλώντας έτσι σοβαρές αναταράξεις στις τιμές και κλονίζοντας την εμπιστοσύνη στην αγορά.

Σήμερα, θα λέγαμε ότι το Bitcoin μοιάζει περισσότερο με τα παραδοσιακά περιουσιακά στοιχεία σε σχέση με τα πρώτα χρόνια του. Καθώς χρησιμοποιείται περισσότερο στο λιανικό εμπόριο,

τα χρηματοοικονομικά και την πολιτική, η τιμή και οι συναλλαγές του επηρεάζονται από περισσότερους παράγοντες. Επίσης, οι θεσμικές επενδύσεις σε κρυπτονομίσματα αυξάνονται συνεχώς, ενισχύοντας έτσι την κερδοσκοπία. Αυτοί οι λόγοι λοιπόν, κάνουν τους παράγοντες που επηρεάζουν τις συναλλαγές του σήμερα να διαφέρουν από εκείνους στις αρχές του. Παρακάτω δίνονται μερικοί από αυτούς τους λόγους:

1. Σήμερα, το Bitcoin υπόκειται σε περισσότερους κανονισμούς από ό,τι στο παρελθόν. Με την πάροδο του χρόνου, αυξάνεται η κατανόηση των κρυπτονομισμάτων και έτσι τα κράτη εντείνουν τους ελέγχους και παράλληλα εισάγουν νέους κανονισμούς. Όμως, οι αλλαγές στους κανονισμούς μπορούν να επηρεάσουν την τιμή του Bitcoin. Για παράδειγμα, η αξία του μπορεί να αλλάξει αν μια χώρα αποφασίσει να το απαγορεύσει ή αν γίνει πιο δημοφιλές σε κάποια άλλη.
2. Η παγκόσμια οικονομική κατάσταση επηρεάζει άμεσα την αξία και τις συναλλαγές του Bitcoin. Για παράδειγμα, άνθρωποι που ζουν σε χώρες με υπερπληθωρισμό στρέφονται στα κρυπτονομίσματα ως μέσο προστασίας από τον πληθωρισμό. Χαρακτηριστικό παράδειγμα αποτελεί η Βενεζουέλα, όπου εξαιτίας της οικονομικής κρίσης που υπέστη, οδηγήθηκε σε ρεκόρ συναλλαγών σε Bitcoin μέσω της πλατφόρμας LocalBitcoins, χρησιμοποιώντας το μπολίβαρ (νόμισμα της Βενεζουέλας).
3. Η αυξημένη αποδοχή του Bitcoin από μεγάλες εταιρείες, όπως η Paypal, η Visa και η Mastercard, βοηθούν στην ενίσχυση της εμπιστοσύνης των επενδυτών, με αποτέλεσμα την άνοδο της τιμής του. Αντίθετα, η απόσυρση αυτής της στήριξης μπορεί να οδηγήσει σε πωλήσεις, όπως συνέβη όταν ο Elon Musk ανακοίνωσε το Μάϊο του 2021 ότι η Tesla θα σταματήσει να δέχεται Bitcoin ως μέσο πληρωμής. Εκείνη την ημέρα, η τιμή του Bitcoin έπεσε από σχεδόν 55.000 δολάρια ανά BTC σε περίπου 48.500.

1.3. Η Εξέλιξη των Ψηφιακών Νομισμάτων

1.3.1. Κατηγορίες των Ψηφιακών Νομισμάτων

Τα ψηφιακά νομίσματα έχουν σημειώσει σημαντική εξέλιξη από την εμφάνιση του Bitcoin το 2009 και έπειτα, καθώς έχουν αλλάξει τον τρόπο με τον οποίο αντιλαμβανόμαστε τις χρηματοοικονομικές συναλλαγές και τη φύση του χρήματος. Η τεχνολογία Blockchain που στηρίζει το Bitcoin κέρδισε γρήγορα την προσοχή προγραμματιστών και επενδυτών, οδηγώντας στη δημιουργία πολλών νέων ψηφιακών νομισμάτων, γνωστών ως "Altcoins" (Wadsworth, A. (2018)). Αυτά τα νέα νομίσματα, με βάση την ανοιχτή φύση του κώδικα του Bitcoin, αντιπροσωπεύουν μια συνεχόμενη καινοτομία στον χώρο των κρυπτονομισμάτων. Παρακάτω παρουσιάζονται οι πιο σημαντικές κατηγορίες ψηφιακών νομισμάτων:

1. Κρυπτονομίσματα (Cryptocurrencies)

Τα κρυπτονομίσματα αποτελούν μια κατηγορία ψηφιακών νομισμάτων που χρησιμοποιούν κρυπτογραφία για την ασφάλεια των συναλλαγών. Το πιο γνωστό παράδειγμα είναι το Bitcoin, το οποίο ήταν το πρώτο ψηφιακό νόμισμα που κυκλοφόρησε. Άλλα παραδείγματα περιλαμβάνουν το Ethereum, το Binance Coin και το Solana, τα οποία είναι γνωστά και ως Altcoins. Επίσης, πρέπει να τονίσουμε ότι, ενώ όλα τα κρυπτονομίσματα είναι ψηφιακά νομίσματα, το αντίστροφο δεν ισχύει.

Πιο συγκεκριμένα, τα κρυπτονομίσματα είναι αποκεντρωμένα (Lim, J.W. (2015)) και βασίζονται στην Τεχνολογία Κατανεμημένου Καθολικού (Distributed Ledger Technology - DLT), κατά την οποία ασφαλή μητρώα διατηρούνται συγχρονισμένα μόνιμα ανάμεσα σε πολλούς συμμετέχοντες. Επιπλέον, επιτρέπουν άμεσες διαδικτυακές πληρωμές μεταξύ δύο μερών χωρίς τη μεσολάβηση τρίτων, χρησιμοποιώντας τεχνικές κρυπτογράφησης για την μεταφορά (Wadsworth, A. (2018)). Τέλος, θεωρούνται νομίσματα χωρίς χρέος, με σταθερό ρυθμό ανάπτυξης και περιορισμένη προσφορά, ενώ παράλληλα μπορούν να επιβάλλουν δημοσιονομική πειθαρχία στις κυβερνήσεις.

Δύο χαρακτηριστικά παραδείγματα κρυπτονομισμάτων είναι το Litecoin και το Ethereum. Συγκεκριμένα, το Litecoin δημιουργήθηκε το 2011, από τον πρώην υπάλληλο της Google, Charlie Lee. Αυτό το κρυπτονόμισμα, πρόσφερε πιο γρήγορες συναλλαγές και μια διαφορετική προσέγγιση στον αλγόριθμο εξόρυξης, διαφοροποιώντας το από το Bitcoin. Αργότερα, το 2015,

δημιουργήθηκε το Ethereum, που εισήγαγε την έννοια των έξυπνων συμβολαίων (smart contracts), επεκτείνοντας τη λειτουργικότητα του blockchain πέρα από τις απλές χρηματικές συναλλαγές.

2. Fiat Currency (Παραστατικό νόμισμα)

Το παραστατικό νόμισμα, είναι ένα είδος χρήματος που καθιερώνεται από την κυβέρνηση και δεν έχει δική του εγγενή αξία. Με άλλα λόγια, πρόκειται για το επίσημο εθνικό νόμισμα που εκδίδεται από την κυβέρνηση ή την κεντρική τράπεζα μιας χώρας.

Οι κεντρικές τράπεζες εκδίδουν παραστατικά μετρητά εκ μέρους των κυβερνήσεων, τα οποία αναγνωρίζονται ως νόμιμο χρήμα για συναλλαγές. Οι άνθρωποι το εμπιστεύονται, καθώς πιστεύουν ότι η κυβέρνηση θα παραμείνει οικονομικά σταθερή και δεν θα χρεοκοπήσει. Επιπλέον, το παραστατικό νόμισμα χρησιμοποιείται ευρέως επειδή είναι αξιόπιστη μονάδα μέτρησης, μέσο συναλλαγής και αποθήκευσης αξίας, ενώ μπορεί επίσης να χρησιμοποιηθεί για την πληρωμή φόρων (Wadsworth, A. (2018)). Τέλος, το φυσικό χρήμα περιλαμβάνει δύο βασικά χαρακτηριστικά: αφενός είναι νόμισμα που εκδίδεται από την κυβέρνηση και θεωρείται νόμιμο, και αφετέρου δεν συνδέεται με την αξία κάποιου απτού περιουσιακού στοιχείου, όπως ο χρυσός.

3. Stablecoins

Τα stablecoins (σταθερά νομίσματα) είναι ένας τύπος κρυπτονομίσματος που σχεδιάστηκε για να διατηρεί μια σταθερή αξία, συνήθως συνδεδεμένη με την αξία ενός συγκεκριμένου παραδοσιακού νομίσματος, όπως το δολάριο ή το ευρώ, προσφέροντας έτσι σταθερότητα στις συναλλαγές. Επιπλέον, διαφέρουν σημαντικά στις νομισματικές αρχές και τους τρόπους έκδοσής τους.

Συναντώνται σε τρεις κύριες μορφές: i) έχουν ισοτιμία ένα προς ένα με επίσημα παραστατικά νομίσματα, ii) υποστηρίζονται από χρηματοοικονομικά περιουσιακά στοιχεία αντί για παραστατικά νομίσματα και iii) η έκδοσή τους ελέγχεται από έναν προηγμένο αλγόριθμο (Maire et al. (2019)).

4. e-Money

Το ηλεκτρονικό χρήμα (e-Money), σύμφωνα με τους Peters et al. το 2015, είναι η νομισματική αξία που αποθηκεύεται ψηφιακά και αντιπροσωπεύει ένα δικαίωμα πληρωμής. Εκδίδεται από έναν πάροχο σε αντάλλαγμα χρημάτων και μπορεί να χρησιμοποιηθεί για συναλλαγές από τρίτους, εκτός από τον ίδιο τον πάροχο. Αυτό περιλαμβάνει προπληρωμένες κάρτες και ηλεκτρονικούς λογαριασμούς που χρησιμοποιούνται στο διαδίκτυο. Συνήθως, το e-Money διατηρεί την ίδια νομισματική μονάδα με το αντίστοιχο παραστατικό νόμισμα που χρησιμοποιήθηκε για την έκδοσή του. Μπορεί επίσης να θεωρηθεί ως το ψηφιακό αντίστοιχο μιας προπληρωμένης κάρτας. Επίσης, ορισμένα είδη e-Money περιλαμβάνουν και stablecoins, που διασφαλίζουν σταθερότητα αξίας. Τέλος, το e-Money διευκολύνει τις συναλλαγές, καθώς μπορεί να χρησιμοποιηθεί άμεσα και εύκολα μέσω εφαρμογών σε κινητές συσκευές, επιτρέποντας άνετες συναλλαγές μεταξύ ατόμων και επιχειρήσεων.

5. Non-Convertible virtual currencies (Μη-μετατρέψιμα εικονικά νομίσματα)

Αυτά τα νομίσματα χρησιμοποιούνται αποκλειστικά σε έναν συγκεκριμένο τομέα ή εικονικό περιβάλλον, όπου η χρήση τους διέπεται από συγκεκριμένους κανόνες και δεν είναι δυνατή η ανταλλαγή τους με παραστατικό νόμισμα (Lim, J.W. (2015)).

1.3.2. Η Άνοδος των ICOs και η Ρυθμιστική Αντίδραση

Καθώς τα κρυπτονομίσματα έγιναν πιο δημοφιλή, πολλές εταιρείες άρχισαν να χρησιμοποιούν την τεχνολογία blockchain για να συγκεντρώσουν κεφάλαια μέσω μιας διαδικασίας γνωστής ως Initial Coin Offering (ICO). Τα ICOs αποτέλεσαν μια καινοτόμο μορφή χρηματοδότησης επιχειρηματικών κεφαλαίων μέσω κρυπτονομισμάτων, όπου οι επενδυτές αγόραζαν τα tokens (ψηφιακή μονάδα αξίας που εκδίδεται μέσω τεχνολογίας Blockchain) μιας νέας εταιρείας με την προσδοκία ότι η αξία τους θα αυξάνεται καθώς η εταιρεία θα αναπτύσσεται (Campino, J., Brochado, A. & Rosa, Á. (2022)).
Ουσιαστικά, τα ICOs μπορούν να οριστούν ως ανοιχτές εκκλήσεις για χρηματοδότηση, οι οποίες προωθούνται από οργανισμούς, εταιρείες και επιχειρηματίες με στόχο τη συγκέντρωση κεφαλαίων μέσω κρυπτονομισμάτων. Σε αντάλλαγμα, οι επενδυτές λαμβάνουν ένα token που μπορεί να πωληθεί στο διαδίκτυο ή να χρησιμοποιηθεί στο μέλλον για την απόκτηση προϊόντων ή υπηρεσιών, καθώς και, σε ορισμένες περιπτώσεις, για την απόκτηση κερδών. Έτσι, το φαινόμενο των ICOs γνώρισε τεράστια άνοδο, καθώς μέχρι το τέλος του 2017, επέτρεψε στις νεοφυείς επιχειρήσεις παγκοσμίως να συγκεντρώσουν περισσότερα από 5.3 δισεκατομμύρια δολάρια (Adhami, S. et al. (2018)).

Ωστόσο, παρά την επιτυχία τους, η ραγδαία άνοδος τους δεν συνοδεύτηκε από την απαραίτητη ρύθμιση, γεγονός που οδήγησε σε πολλές περιπτώσεις απάτης και σημαντικών οικονομικών απωλειών για τους επενδυτές. Αυτή η έλλειψη ρύθμισης προκάλεσε την αντίδραση κυβερνήσεων και ρυθμιστικών αρχών, οι οποίες άρχισαν να εξετάζουν τρόπους για να ελέγξουν τα ICOs και την αγορά κρυπτονομισμάτων γενικότερα, με στόχο την προστασία των επενδυτών και τη διασφάλιση της σταθερότητας των χρηματοοικονομικών αγορών. Έτσι λοιπόν, πολλές χώρες άρχισαν να θεσπίζουν κανονιστικά μέτρα για την παρακολούθηση και τον έλεγχο των ICOs. Ορισμένες από αυτές, όπως οι Ηνωμένες Πολιτείες, άρχισαν να αντιμετωπίζουν τα tokens ως χρηματοοικονομικά προϊόντα που υπόκεινται σε νομοθεσίες περί τίτλων, ενώ άλλες, όπως η Κίνα, προχώρησαν σε πλήρη απαγόρευση τους. Αυτές οι ρυθμιστικές παρεμβάσεις είχαν ως στόχο την προστασία των επενδυτών, την αποτροπή της χρήσης των ICOs για ξέπλυμα χρήματος και άλλες παράνομες δραστηριότητες, καθώς και τη διασφάλιση της ομαλής λειτουργίας των αγορών.

Συνοψίζοντας, θα λέγαμε ότι η άντληση κεφαλαίων μέσω ICOs μπορεί να θεωρηθεί ως ένα κρίσιμο σημείο στην ιστορία των κρυπτονομισμάτων, το οποίο οδήγησε στην ανάγκη για πιο ώριμη και σταθερή ρύθμιση του τομέα, επηρεάζοντας την εξέλιξη των ψηφιακών αγορών και την εμπιστοσύνη των επενδυτών σε αυτές. Παράλληλα, προσέφεραν μια εναλλακτική λύση στην παραδοσιακή άντληση κεφαλαίων, επιτρέποντας στις εταιρείες να συγκεντρώσουν κεφάλαια γρήγορα και συχνά χωρίς τους περιορισμούς των παραδοσιακών αγορών. Ωστόσο, αυτή η ελευθερία τα κατέστησε ευάλωτα, με αποτέλεσμα πολλοί επενδυτές να χάσουν τα χρήματά τους χωρίς δυνατότητα επανόρθωσης. Παρά τα προβλήματα αυτά, τα ICOs συνέβαλαν σημαντικά στην ανάπτυξη έργων ανοικτού κώδικα και αποκεντρωμένων επιχειρήσεων, δημιουργώντας μια ενσωματωμένη πελατειακή βάση και θετικά δικτυακά αποτελέσματα (Giudici & Rossi-Lamastra, 2018).

1.3.3. Εισαγωγή των Κεντρικών Τραπεζών στα Ψηφιακά Νομίσματα

Αντιλαμβανόμενες τον αντίκτυπο που θα μπορούσαν να έχουν τα ψηφιακά νομίσματα στην οικονομική σταθερότητα και τη νομισματική πολιτική, πολλές κεντρικές τράπεζες άρχισαν να διερευνούν την ιδέα της δημιουργίας Κεντρικής Τράπεζας Ψηφιακών Νομισμάτων (CBDCs), ώστε να παρέχουν ψηφιακό νόμισμα στο κοινό. Ειδικότερα, το ψηφιακό νόμισμα κεντρικής τράπεζας (CBDC) είναι ψηφιακό χρήμα, που αποθηκεύεται ηλεκτρονικά και ελέγχεται από τις κεντρικές τράπεζες. Αυτό το ψηφιακό νόμισμα μπορεί να χρησιμοποιηθεί από τους πολίτες για πληρωμές, όπως ακριβώς χρησιμοποιείται το φυσικό χρήμα, προσφέροντας έτσι νέες δυνατότητες στον τρόπο διαχείρισης των χρημάτων από το κοινό.

Μία προσέγγιση αυτής της ιδέας, είναι η δημιουργία κεντρικοποιημένων λογαριασμών, στους οποίους οι πολίτες θα μπορούν να αποθηκεύουν ψηφιακό χρήμα απευθείας στην κεντρική τράπεζα, κάτι που σήμερα είναι δυνατό μόνο για συγκεκριμένα χρηματοπιστωτικά ιδρύματα. Με αυτόν τον τρόπο, η κεντρική τράπεζα θα λειτουργεί ως ένας φορέας που προσφέρει λογαριασμούς στο ευρύ κοινό, επιτρέποντας τους να πραγματοποιούν πληρωμές μέσω του συστήματός της. Εναλλακτικά, μια άλλη προσέγγιση είναι η έκδοση ψηφιακού νομίσματος με τρόπο παρόμοιο με τη διανομή φυσικού χρήματος, δηλαδή με έναν αποκεντρωμένο τρόπο (Engert, W. and Fung, B. (2017)).

Υπάρχουν διάφοροι λόγοι που μπορεί να ωθήσουν μια κεντρική τράπεζα να εξετάσει τη δημιουργία CBDC για το ευρύ κοινό. Μερικοί από αυτούς είναι:

1. Εξασφάλιση επαρκούς ποσότητας χρήματος της κεντρικής τράπεζας για το κοινό και διατήρηση των εσόδων από το δικαίωμα εκτύπωσης χρήματος της
2. Μείωση του κατώτατου ορίου των επιτοκίων και υποστήριξη μη συμβατικής νομισματικής πολιτικής
3. Μείωση του συνολικού κινδύνου και βελτίωση της χρηματοοικονομικής σταθερότητας
4. Αύξηση του ανταγωνισμού στις πληρωμές
5. Προώθηση της χρηματοοικονομικής ένταξης
6. Παρεμπόδιση της εγκληματικής δραστηριότητας

Τα τελευταία χρόνια, έχει υπάρξει εκτεταμένη συζήτηση σχετικά με τις πιθανές επιπτώσεις της εισαγωγής των CBDC στις οικονομίες και το κατά πόσο θα πρέπει να καταργηθούν τα μετρητά (Davoodalhosseini, S.M. (2022)). Ορισμένες κεντρικές τράπεζες έχουν ήδη ξεκινήσει τη διαδικασία λήψης αποφάσεων για το αν θα προχωρήσουν στην εισαγωγή ενός CBDC στις αντίστοιχες οικονομίες τους. Ένα χαρακτηριστικό παράδειγμα είναι η Riksbank της Σουηδίας, η οποία εξέδωσε το e-krona, ένα ψηφιακό σουηδικό νόμισμα, το οποίο πλέον βρίσκεται στην 4η φάση δοκιμών, με στόχο να διερευνήσει πώς θα μπορούσε να χρησιμοποιηθεί από το ευρύ κοινό. Η Κίνα έχει επίσης αναπτύξει το e-yuan (e-CNY), στο πλαίσιο της στρατηγικής της για την ενίσχυση της ψηφιοποίησης της οικονομίας και τη μείωση της εξάρτησης από το φυσικό χρήμα. Καταλήγοντας, τρεις χώρες έχουν προχωρήσει πλήρως στην εισαγωγή ενός CBDC: οι Μπαχάμες με το Sand Dollar, η Τζαμάικα με το JAM-DEX και η Νιγηρία με το eNaira, καθιστώντας τα από τα πρώτα έθνη που υιοθέτησαν πλήρως ψηφιακά νομίσματα.

1.4. Τεχνολογικές Προκλήσεις

Μπορεί η τεχνολογία πίσω από τα ψηφιακά νομίσματα και το blockchain να είναι πρωτοποριακή, ωστόσο υπάρχουν και αρκετές τεχνολογικές προκλήσεις, που πρέπει να αντιμετωπιστούν προκειμένου να εξασφαλιστεί η ευρεία αποδοχή και η μακροπρόθεσμη βιωσιμότητά τους. Οι προκλήσεις αυτές ποικίλουν από την κλίμακα και την απόδοση των δικτύων μέχρι την ασφάλεια και την ιδιωτικότητα των χρηστών. Παρακάτω, αναλύονται οι κύριες τεχνολογικές προκλήσεις που αντιμετωπίζουν τα ψηφιακά νομίσματα.

Ασφάλεια και Ιδιωτικότητα των χρηστών

Η ασφάλεια αποτελεί βασικό στοιχείο για την αποδοχή και την εμπιστοσύνη των χρηστών στα ψηφιακά νομίσματα, ωστόσο, αντιμετωπίζει σημαντικές προκλήσεις που κυμαίνονται από επιθέσεις στον κώδικα του blockchain έως την κλοπή κρυπτονομισμάτων από τα ψηφιακά πορτοφόλια των χρηστών. Η προστασία των ψηφιακών πορτοφολιών και των ιδιωτικών κλειδιών είναι εξίσου κρίσιμη, καθώς έχουν καταγραφεί πολλά περιστατικά απώλειας νομισμάτων λόγω κλοπών ή επιθέσεων phishing, όπου τα ιδιωτικά κλειδιά υποκλέπτονται. Αυτές οι απώλειες είναι συνήθως μη αναστρέψιμες, δεδομένου ότι δεν υπάρχει κεντρική αρχή που να μπορεί να ακυρώσει μια συναλλαγή ή να επαναφέρει τα κλεμμένα νομίσματα.

Αν και τα κρυπτονομίσματα βασίζονται σε κρυπτογραφικές τεχνικές για να διασφαλίσουν την ακεραιότητα των συναλλαγών και την προστασία των χρηστών, παραμένουν ευάλωτα σε επιθέσεις. Ένα χαρακτηριστικό παράδειγμα αποτελεί η επίθεση 51%, κατά την οποία ένας κακόβουλος παράγοντας αποκτά τον έλεγχο της πλειοψηφίας (πάνω από το 50%) της υπολογιστικής ισχύος του δικτύου, επιτρέποντας την επανεγγραφή της αλυσίδας και τη διπλή δαπάνη νομισμάτων. Παρόλο που οι επιθέσεις αυτές είναι εξαιρετικά δύσκολες και δαπανηρές να πραγματοποιηθούν σε μεγάλα δίκτυα, όπως το Bitcoin, εξακολουθούν να αποτελούν πραγματική απειλή για μικρότερα δίκτυα με λιγότερους πόρους.

Επιπλέον, ένα πολύ σημαντικό ζήτημα που πρέπει να ληφθεί υπόψη είναι η προστασία της ιδιωτικότητας και της ανωνυμίας στις συναλλαγές με ψηφιακά νομίσματα. Ενώ τα περισσότερα

ψηφιακά νομίσματα, όπως το Bitcoin, παρέχουν κάποιο βαθμό ανωνυμίας, δεν εξασφαλίζουν πλήρη ιδιωτικότητα. Αντίθετα, κρυπτονομίσματα όπως το Monero και το Zcash, έχουν σχεδιαστεί ειδικά για να παρέχουν αυξημένη προστασία ιδιωτικότητας στις συναλλαγές, αξιοποιώντας τεχνολογίες όπως οι zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). Αυτές οι τεχνολογίες επιτρέπουν την επιβεβαίωση των συναλλαγών χωρίς να αποκαλύπτονται οι λεπτομέρειες τους, διασφαλίζοντας έτσι την πλήρη ιδιωτικότητα των χρηστών.

Καταλήγοντας, να τονίσουμε ότι, παρόλο που οι συναλλαγές με κρυπτονομίσματα θεωρούνται ανώνυμες, στην πραγματικότητα οι περισσότερες συναλλαγές είναι ψευδώνυμες, με τις διευθύνσεις των πορτοφολιών να μπορούν να εντοπιστούν πίσω στους ιδιοκτήτες τους.

Επεκτασιμότητα και Απόδοση

Μία άλλη σημαντική πρόκληση που αντιμετωπίζουν τα ψηφιακά νομίσματα είναι η επεκτασιμότητα, δηλαδή η ικανότητα του δικτύου να διαχειρίζεται αυξανόμενο αριθμό συναλλαγών χωρίς να μειώνεται η απόδοσή του. Το Bitcoin, για παράδειγμα, μπορεί να επεξεργαστεί περίπου 7 συναλλαγές ανά δευτερόλεπτο (TPS), ενώ το Ethereum μπορεί να φτάσει μέχρι τις 30 TPS.

Αυτή η μεγάλη διαφορά στην απόδοση δημιουργεί σοβαρά εμπόδια για την ευρεία αποδοχή των ψηφιακών νομισμάτων ως καθημερινών εργαλείων συναλλαγών. Η χαμηλή δυνατότητα επεξεργασίας συναλλαγών οδηγεί σε υψηλές χρεώσεις και μεγαλύτερους χρόνους επεξεργασίας, καθιστώντας τα συστήματα λιγότερο αποδοτικά και οικονομικά για τους χρήστες. Το πρόβλημα αυτό γίνεται ιδιαίτερα εμφανές κατά τη διάρκεια περιόδων έντονης ζήτησης, όπως όταν το δίκτυο είναι υπερφορτωμένο λόγω αυξημένου όγκου συναλλαγών.

Η ανάγκη για κλιμάκωση των δικτύων blockchain έχει οδηγήσει στην ανάπτυξη πολλαπλών λύσεων που στοχεύουν στη βελτίωση της αποδοτικότητας και στην αντιμετώπιση των προκλήσεων που σχετίζονται με την επεξεργασία μεγάλου όγκου συναλλαγών. Η επεκτασιμότητα είναι ζωτικής σημασίας για τη μελλοντική βιωσιμότητα των κρυπτονομισμάτων και τη δυνατότητά τους να ανταγωνιστούν τα παραδοσιακά

χρηματοοικονομικά συστήματα. Γι' αυτόν τον λόγο, έχουν προταθεί δύο κύριες κατηγορίες λύσεων.

Η πρώτη αφορά την αναβάθμιση του ίδιου του πρωτοκόλλου του blockchain, γνωστή και ως λύσεις Layer 1. Ένα χαρακτηριστικό παράδειγμα είναι το Segregated Witness (SegWit), το οποίο εφαρμόστηκε στο Bitcoin το 2017, επιτρέποντας μεγαλύτερη αποδοτικότητα στην αποθήκευση των συναλλαγών και αυξάνοντας τον αριθμό των συναλλαγών ανά block. Η δεύτερη κατηγορία, που περιλαμβάνει τις λύσεις Layer 2, επικεντρώνεται στη μεταφορά των συναλλαγών εκτός της κύριας αλυσίδας (off-chain) για να αποσυμφορηθεί το κεντρικό δίκτυο. Ένα από τα πιο γνωστά παραδείγματα είναι το Lightning Network για το Bitcoin, το οποίο επιτρέπει σχεδόν άμεσες συναλλαγές με χαμηλότερα τέλη, χωρίς να καταγράφονται όλες οι συναλλαγές στο κύριο blockchain. Αντίστοιχα, το Ethereum αξιοποιεί λύσεις όπως τα Optimistic Rollups, που επίσης συμβάλλουν στην αύξηση της δυνατότητας επεξεργασίας συναλλαγών χωρίς να επιβαρύνεται το κεντρικό δίκτυο.

Κατανάλωση Ενέργειας

Η υψηλή κατανάλωση ενέργειας που απαιτείται για την εξόρυξη κρυπτονομισμάτων, ιδιαίτερα σε δίκτυα που χρησιμοποιούν τον αλγόριθμο Proof of Work (PoW), όπως το Bitcoin, έχει εγείρει σοβαρές ανησυχίες σχετικά με το περιβαλλοντικό τους αποτύπωμα. Η εξόρυξη κρυπτονομισμάτων απαιτεί τεράστια υπολογιστική ισχύ, η οποία μεταφράζεται σε σημαντική κατανάλωση ηλεκτρικής ενέργειας, γεγονός που έχει προκαλέσει έντονη κριτική από κυβερνήσεις και περιβαλλοντικές οργανώσεις, οι οποίες ζητούν άμεσες λύσεις για τη μείωση αυτής της κατανάλωσης.

Μία από τις κύριες προσεγγίσεις για την αντιμετώπιση αυτού του ζητήματος είναι η μετάβαση σε αλγόριθμους συναίνεσης που καταναλώνουν λιγότερη ενέργεια, όπως ο Proof of Stake (PoS). Το Ethereum, για παράδειγμα, πραγματοποίησε το 2022 τη μετάβασή του από τον PoW στον PoS μέσω της αναβάθμισης γνωστής ως The Merge, μειώνοντας δραστικά την ενεργειακή κατανάλωση του δικτύου. Επιπλέον, άλλες προτεινόμενες λύσεις περιλαμβάνουν τη χρήση ανανεώσιμων πηγών ενέργειας για την εξόρυξη κρυπτονομισμάτων και τη βελτιστοποίηση της αποδοτικότητας στις εξορυκτικές διαδικασίες.

Συνοψίζοντας, οι τεχνολογικές προκλήσεις που αντιμετωπίζουν τα ψηφιακά νομίσματα είναι σημαντικές, αλλά η συνεχής έρευνα και ανάπτυξη στον τομέα αυτόν υπόσχονται να επιφέρουν τις απαραίτητες βελτιώσεις και αναβαθμίσεις. Η επιτυχία των ψηφιακών νομισμάτων εξαρτάται από την ικανότητα των τεχνολογιών να εξελίσσονται και να προσαρμόζονται στις ανάγκες των χρηστών και της παγκόσμιας οικονομίας.

1.5. Επιδράσεις των Ψηφιακών Νομισμάτων στην Παγκόσμια Οικονομία

Τα ψηφιακά νομίσματα, από την εμφάνιση του Bitcoin, έχουν αρχίσει να διαμορφώνουν νέα δεδομένα στην παγκόσμια οικονομία. Καθώς η υιοθέτηση και η χρήση τους επεκτείνεται, οι επιδράσεις τους γίνονται όλο και πιο αισθητές σε διάφορους τομείς, από τις χρηματοοικονομικές αγορές έως τις διακρατικές συναλλαγές. Επιπλέον, η δυνατότητα που προσφέρουν για γρήγορες, ασφαλείς και αποκεντρωμένες συναλλαγές αμφισβητεί τα παραδοσιακά χρηματοοικονομικά συστήματα, με αποτέλεσμα να προκαλούν σημαντικές αλλαγές στον τρόπο με τον οποίο λειτουργούν οι οικονομίες σε παγκόσμιο επίπεδο. Συνεπώς, είναι κρίσιμο να αναλύσουμε αυτές τις επιδράσεις για να κατανοήσουμε τις ευκαιρίες που προκύπτουν από την αυξανόμενη χρήση των ψηφιακών νομισμάτων. Μερικές από τις πιο σημαντικές είναι:

Αλλαγές στο Χρηματοπιστωτικό Σύστημα

- **Νέες επενδυτικές ευκαιρίες**: Τα ψηφιακά νομίσματα έχουν δημιουργήσει μια νέα κατηγορία περιουσιακών στοιχείων, προσελκύοντας επενδυτές που αναζητούν υψηλές αποδόσεις. Αυτό έχει οδηγήσει στη δημιουργία νέων επενδυτικών προϊόντων, όπως τα ETFs κρυπτονομισμάτων και τα παράγωγα που βασίζονται σε κρυπτονομίσματα, δίνοντας στους επενδυτές περισσότερες επιλογές διαφοροποίησης των χαρτοφυλακίων τους.
- **Αυξημένη μεταβλητότητα**: Τα κρυπτονομίσματα είναι γνωστά για την έντονη αστάθειά τους, με τις τιμές τους να παρουσιάζουν μεγάλες διακυμάνσεις σε σύντομο χρονικό

διάστημα. Αυτή η μεταβλητότητά έχει προσελκύσει το ενδιαφέρον κερδοσκόπων, ενώ παράλληλα έχει εγείρει ανησυχίες για τους κινδύνους που ενδέχεται να αντιμετωπίσουν οι επενδυτές. Επίσης, οι μεγάλες διακυμάνσεις των τιμών έχουν αντίκτυπο στις παραδοσιακές χρηματοοικονομικές αγορές, καθώς η αυξανόμενη διασύνδεση μεταξύ των δύο αγορών μπορεί να επηρεάσει την παγκόσμια χρηματοοικονομική σταθερότητα.

- **Αύξηση του θεσμικού ενδιαφέροντος**: Τα τελευταία χρόνια, παρατηρείται αυξημένο ενδιαφέρον από θεσμικούς επενδυτές, όπως επενδυτικά ταμεία, τράπεζες και ασφαλιστικές εταιρείες, για τα ψηφιακά νομίσματα. Αυτό το ενδιαφέρον έχει συμβάλει στην ώθηση των τιμών των κρυπτονομισμάτων και στην ενίσχυση της νομιμοποίησής τους ως επενδυτικών εργαλείων. Ωστόσο, η είσοδος θεσμικών επενδυτών έχει επίσης οδηγήσει σε αυστηρότερη ρύθμιση και εποπτεία από τις κυβερνήσεις και τις ρυθμιστικές αρχές.
- **Δημιουργία νέων αγορών-πλατφόρμων**: Η άνοδος των κρυπτονομισμάτων έχει οδηγήσει στη δημιουργία νέων αγορών και πλατφόρμων συναλλαγών, που επιτρέπουν στους χρήστες να αγοράζουν, να πωλούν και να ανταλλάσσουν ψηφιακά νομίσματα. Αυτές οι πλατφόρμες λειτουργούν παράλληλα με τις παραδοσιακές χρηματοοικονομικές αγορές και προσφέρουν νέες δυνατότητες αλλά και προκλήσεις, όπως η ανάγκη για ενισχυμένα μέτρα ασφαλείας και η αντιμετώπιση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες.
- **Αναδιαμόρφωση της δυναμικής της αγοράς**: Τα ψηφιακά νομίσματα έχουν εισαγάγει νέους τρόπους αλληλεπίδρασης στις χρηματοοικονομικές αγορές, καθώς είναι αποκεντρωμένα και λειτουργούν χωρίς την ανάγκη μεσάζοντα, όπως οι τράπεζες. Αυτό έχει οδηγήσει σε μια αναδιαμόρφωση της δυναμικής της αγοράς, όπου οι τράπεζες πρέπει να προσαρμοστούν στις νέες συνθήκες για να παραμείνουν ανταγωνιστικές.

<u>Επιδράσεις στις διακρατικές συναλλαγές</u>

Χάρη στην αποκεντρωμένη φύση τους, τα ψηφιακά νομίσματα επιτρέπουν ταχύτερες και φθηνότερες διασυνοριακές συναλλαγές, παρακάμπτοντας τους παραδοσιακούς μεσάζοντες και μειώνοντας τις προμήθειες. Αυτό είναι ιδιαίτερα σημαντικό για περιοχές με περιορισμένη πρόσβαση σε τραπεζικές υπηρεσίες. Πιο αναλυτικά, έχουμε:

- **Ευκολότερες και φθηνότερες διασυνοριακές συναλλαγές**: Σε αντίθεση με τις παραδοσιακές μεθόδους, όπως οι διεθνείς τραπεζικές μεταφορές μέσω SWIFT, οι οποίες

μπορεί να χρειαστούν αρκετές ημέρες και να περιλαμβάνουν υψηλές προμήθειες, τα ψηφιακά νομίσματα επιτρέπουν την άμεση μεταφορά χρημάτων με ελάχιστο κόστος. Αυτό είναι ιδιαίτερα ωφέλιμο για άτομα και επιχειρήσεις που πραγματοποιούν συχνά διασυνοριακές συναλλαγές, καθώς μειώνει τα έξοδα και επιταχύνει τη διαδικασία.

- **Αποκέντρωση και ανεξαρτησία από τράπεζες**: Οι διακρατικές συναλλαγές με ψηφιακά νομίσματα δεν εξαρτώνται από μεσάζοντες, όπως οι τράπεζες. Αυτό σημαίνει ότι οι συναλλαγές μπορούν να πραγματοποιηθούν οποιαδήποτε στιγμή, ανεξάρτητα από τις ώρες λειτουργίας των τραπεζών ή τους τοπικούς κανονισμούς. Αυτή η ανεξαρτησία από τις παραδοσιακές δομές κάνει τις συναλλαγές πιο προσβάσιμες σε όλους.
- **Πρόσβαση σε αγορές με περιορισμένη τραπεζική υποδομή**: Σε χώρες με ανεπτυγμένα ή περιορισμένα τραπεζικά συστήματα, τα ψηφιακά νομίσματα παρέχουν έναν τρόπο για να πραγματοποιούνται διεθνείς πληρωμές χωρίς την ανάγκη πρόσβασης σε παραδοσιακές τραπεζικές υπηρεσίες.
- **Μείωση συναλλαγματικού κινδύνου**: Οι παραδοσιακές διακρατικές συναλλαγές συχνά περιλαμβάνουν μετατροπή νομισμάτων, η οποία υπόκειται σε διακυμάνσεις συναλλαγματικών ισοτιμιών και μπορεί να προκαλέσει πρόσθετο κόστος ή απώλειες. Όμως, με τα ψηφιακά νομίσματα, οι συναλλαγές μπορούν να πραγματοποιηθούν χωρίς την ανάγκη μετατροπής σε διαφορετικά εθνικά νομίσματα, μειώνοντας έτσι τον συναλλαγματικό κίνδυνο.
- **Ενίσχυση της οικονομικής ενσωμάτωσης**: Τα ψηφιακά νομίσματα επιτρέπουν σε άτομα και επιχειρήσεις από διαφορετικές χώρες να συνεργάζονται και να πραγματοποιούν συναλλαγές πιο εύκολα, ανεξαρτήτως του τοπικού τραπεζικού συστήματος. Αυτό προάγει την οικονομική ενσωμάτωση και ενισχύει τις διεθνείς επιχειρηματικές σχέσεις, διευκολύνοντας το εμπόριο και τις επενδύσεις σε παγκόσμιο επίπεδο.

Νομισματική πολιτική και έλεγχος

Η αυξανόμενη δημοτικότητα των ψηφιακών νομισμάτων θέτει προκλήσεις για τις κεντρικές τράπεζες, οι οποίες χάνουν τον απόλυτο έλεγχο της νομισματικής πολιτικής. Αυτό μπορεί να οδηγήσει σε νέες στρατηγικές για την ενσωμάτωση ή τη ρύθμιση των κρυπτονομισμάτων στα παραδοσιακά οικονομικά συστήματα. Ορισμένες από τις προκλήσεις αυτές δίνονται παρακάτω:

- **Μείωση ελέγχου των κεντρικών τραπεζών**: Τα ψηφιακά νομίσματα, ειδικά εκείνα που λειτουργούν σε αποκεντρωμένα δίκτυα όπως το Bitcoin, δεν υπόκεινται στον έλεγχο των κεντρικών τραπεζών. Αυτό σημαίνει ότι οι κεντρικές τράπεζες χάνουν την αποκλειστική τους εξουσία στην έκδοση και διαχείριση του χρήματος, γεγονός που μπορεί να περιορίσει την ικανότητά τους να ελέγχουν τη ροή του χρήματος στην οικονομία και να επηρεάζουν βασικούς οικονομικούς δείκτες, όπως ο πληθωρισμός και τα επιτόκια.
- **Δυσκολίες στην εφαρμογή νομισματικής πολιτικής**: Οι παραδοσιακές μορφές νομισματικής πολιτικής, όπως η ρύθμιση των επιτοκίων και η ποσοτική χαλάρωση, βασίζονται στην κεντρική εξουσία που ασκούν οι κυβερνήσεις και οι κεντρικές τράπεζες πάνω στο εθνικό νόμισμα. Με την άνοδο των ψηφιακών νομισμάτων, οι οποίες δεν ελέγχονται από τις ίδιες τις κεντρικές αρχές, η αποτελεσματικότητα αυτών των πολιτικών μπορεί να μειωθεί, καθώς οι άνθρωποι και οι επιχειρήσεις μπορούν να επιλέξουν να χρησιμοποιούν ψηφιακά νομίσματα αντί για το εθνικό νόμισμα.
- **Αποφυγή ελέγχου κεφαλαίων και φοροδιαφυγή**: Τα ψηφιακά νομίσματα μπορούν να χρησιμοποιηθούν για τη μεταφορά κεφαλαίων εκτός των συνόρων χωρίς την έγκριση των αρχών, παρακάμπτοντας έτσι τα εθνικά μέτρα ελέγχου κεφαλαίων. Αυτό μπορεί να οδηγήσει σε απώλεια εσόδων για το κράτος μέσω της φοροδιαφυγής και να δυσκολέψει τις κυβερνήσεις στην παρακολούθηση και τη ρύθμιση των χρηματοοικονομικών ροών.
- **Ανάγκη για νέους κανονισμούς**: Η άνοδος των ψηφιακών νομισμάτων έχει προκαλέσει την ανάγκη για νέους κανονισμούς που να αντιμετωπίζουν τις προκλήσεις που θέτουν στην παραδοσιακή νομισματική πολιτική. Οι κυβερνήσεις και οι κεντρικές τράπεζες αναζητούν τρόπους να ενσωματώσουν τα ψηφιακά νομίσματα στα υπάρχοντα νομισματικά συστήματα, χωρίς να υπονομεύσουν τη σταθερότητα και την ασφάλεια των εθνικών οικονομιών.

Επιπλέον, σύμφωνα με τη μελέτη "Κεντρική Τράπεζα και Κρυπτονόμισμα", που δημοσιεύθηκε το 2017 από την εταιρεία "Accenture Consulting", τα κρυπτονομίσματα έχουν σημαντικό αντίκτυπο στην οικονομία, με διάφορους τρόπους. Συγκεκριμένα, τα κρυπτονομίσματα:

- Ενισχύουν την οικονομική ανάπτυξη
- Λειτουργούν ως ενισχυτής για το κινητό (mobile) και ψηφιακό εμπόριο
- Διασφαλίζουν την ισορροπία στο χρηματοοικονομικό σύστημα
- Λειτουργούν ως κρυπτο-αποθεματικό νόμισμα

- Παρακολουθούν παραγωγικά την προσφορά χρήματος
- Μειώνουν το κόστος
- Επιτρέπουν την ιχνηλασιμότητα

Τα ψηφιακά νομίσματα έχουν αρχίσει να αναμορφώνουν την παγκόσμια οικονομία, επηρεάζοντας τις χρηματοοικονομικές αγορές, τις διακρατικές συναλλαγές και τη νομισματική πολιτική. Παρά τις σημαντικές ευκαιρίες που προσφέρουν, όπως η μείωση του κόστους και η ενίσχυση της οικονομικής ανάπτυξης, οι προκλήσεις παραμένουν, απαιτώντας προσαρμογή και ρύθμιση.

ΚΕΦΑΛΑΙΟ 2. ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

2.1. Ορισμός και Κύρια Χαρακτηριστικά

Η εξέλιξη της τεχνολογίας έχει οδηγήσει στην εμφάνιση πολλών καινοτομιών τα τελευταία χρόνια. Μια από τις πιο αξιοσημείωτες είναι η τεχνολογία Blockchain, η οποία είναι επίσης γνωστή ως τεχνολογία του ασφαλούς καθολικού και αποτελεί τον πυρήνα της λειτουργίας του Bitcoin, προσελκύοντας το ενδιαφέρον της παγκόσμιας κοινότητας. Επίσης, στον χώρο της πληροφορικής, η Blockchain αναφέρεται συχνά ως η πέμπτη σημαντική καινοτομία στην τεχνολογία (Singh, G., Garg, V. & Tiwari, P. (2021)). Σε γενικές γραμμές, μπορεί να θεωρηθεί ως ένα κατανεμημένο καθολικό εγγραφών, δηλαδή μια κοινόχρηστη βάση δεδομένων που λειτουργεί μέσω ενός συστήματος συναίνεσης, το οποίο επιτρέπει την ασφαλή και αξιόπιστη επικύρωση κάθε συναλλαγής.

Από την εισαγωγή της τεχνολογίας Blockchain το 2008, η έννοια αυτής της τεχνολογίας έχει βρει ποικίλες εφαρμογές και έχει χρησιμοποιηθεί με πολλούς διαφορετικούς τρόπους. Το αυξημένο ενδιαφέρον για την τεχνολογία Blockchain οφείλεται στα ιδιαίτερα χαρακτηριστικά της και στην ικανότητά της να προσφέρει ασφάλεια, ιδιωτικότητα και ακεραιότητα δεδομένων χωρίς την ανάγκη παρέμβασης ενός τρίτου μέρους για τον έλεγχο των συναλλαγών. Το πιο εμφανές αποτέλεσμα αυτής της τεχνολογίας είναι η δημιουργία πολλών κρυπτονομισμάτων. Ωστόσο, είναι σημαντικό να τονιστεί ότι η εφαρμογή της τεχνολογίας Blockchain δεν περιορίζεται μόνο στα κρυπτονομίσματα. Στην πραγματικότητα, είναι πολύ πιο περίπλοκη από την απλή αποθήκευση κατανεμημένου καθολικού και έχει βρει εφαρμογή σε διάφορους τομείς, όπως τα χρηματοοικονομικά, η βιομηχανία, η ιατρική και η εκπαίδευση. Επιπλέον, μπορεί να εφαρμοστεί και σε άλλους τομείς, όπως τα έξυπνα συμβόλαια (smart contracts), οι δημόσιες υπηρεσίες, το Διαδίκτυο των Πραγμάτων (IoT) και οι υπηρεσίες ασφαλείας (Zheng, Z. Et al. (2017)).

Τα μοναδικά πλεονεκτήματα που προσφέρει η Blockchain περιλαμβάνουν αξιοπιστία, συνεργασία, οργάνωση, ταυτοποίηση, εγκυρότητα και διαφάνεια. Ειδικά στον χρηματοοικονομικό τομέα και στις τραπεζικές συναλλαγές, η τεχνολογία Blockchain έχει ήδη καταλάβει κεντρικό ρόλο, ενώ πολλές μεγάλες εταιρείες πειραματίζονται με την εφαρμογή της και σε άλλους τομείς. Συνοπτικά, τα κύρια χαρακτηριστικά της είναι:

- **Αποκέντρωση**: Στα παραδοσιακά κεντρικοποιημένα συστήματα συναλλαγών, κάθε συναλλαγή απαιτεί επικύρωση από μια κεντρική αξιόπιστη αρχή, όπως μια κεντρική τράπεζα, κάτι που συχνά οδηγεί σε αυξημένα κόστη και πιθανά προβλήματα απόδοσης στους κεντρικούς εξυπηρετητές. Αντιθέτως, η τεχνολογία Blockchain δεν απαιτεί μεσάζων.

- **Ασφάλεια**: Είναι εξαιρετικά ασφαλής λόγω της χρήσης προηγμένων κρυπτογραφικών μεθόδων. Κάθε block είναι κρυπτογραφημένο και συνδέεται με το προηγούμενο μέσω ενός ασφαλούς αλγορίθμου Hash, που καθιστά πολύ δύσκολη την αλλοίωση της αλυσίδας.

- **Διαφάνεια**: Προσφέρει υψηλό επίπεδο διαφάνειας, καθώς κάθε κόμβος στο δίκτυο έχει πρόσβαση σε ολόκληρο το ιστορικό των συναλλαγών. Αυτό σημαίνει ότι οποιαδήποτε αλλαγή ή νέα συναλλαγή είναι άμεσα ορατή από όλους τους συμμετέχοντες στο δίκτυο.

- **Ανωνυμία**: Κάθε χρήστης μπορεί να αλληλοεπιδράσει με το blockchain μέσω μιας ηλεκτρονικής διεύθυνσης, η οποία δεν αποκαλύπτει την πραγματική του ταυτότητα. Παρ' όλα αυτά, το blockchain δεν μπορεί να εξασφαλίσει απόλυτη προστασία της ιδιωτικότητας εξαιτίας των ενσωματωμένων περιορισμών του.

- **Αμετάβλητο**: Οι συναλλαγές μπορούν να επαληθευτούν άμεσα και οι άκυρες συναλλαγές εντοπίζονται αμέσως και δεν γίνονται αποδεκτές. Επιπλέον, είναι σχεδόν αδύνατο να διαγραφούν ή να αναιρεθούν συναλλαγές μόλις αυτές περιληφθούν στο blockchain.

- **Συναίνεση**: Χρησιμοποιεί μηχανισμούς συναίνεσης (όπως το Proof of Work (PoW) ή το Proof of Stake (PoS)) για να εξασφαλίσει ότι όλες οι συναλλαγές είναι έγκυρες και ότι όλοι οι κόμβοι συμφωνούν στο τρέχον στάδιο της αλυσίδας.

- **Δυνατότητα Ελέγχου**: Το Bitcoin blockchain αποθηκεύει δεδομένα σχετικά με τα υπόλοιπα των χρηστών χρησιμοποιώντας στο μοντέλο Unspent Transaction Output (UTXO) (Nakamoto, S. (2008)). Κάθε συναλλαγή πρέπει να βασίζεται σε προηγούμενες

αχρησιμοποίητες συναλλαγές. Όταν η τρέχουσα συναλλαγή καταγραφεί στο blockchain, οι αντίστοιχες αχρησιμοποίητες συναλλαγές μετατρέπονται από αχρησιμοποίητες σε χρησιμοποιημένες. Έτσι, οι συναλλαγές μπορούν να επαληθευτούν και να παρακολουθηθούν εύκολα.

Με τα παραπάνω χαρακτηριστικά, μπορεί να μειώσει σημαντικά το κόστος και να βελτιώσει την αποδοτικότητα.

2.1.1. Οι Τύποι Blockchain

Τα τρέχοντα συστήματα blockchain κατατάσσονται γενικά σε τέσσερις κατηγορίες: public blockchain (δημόσιο), private blockchain (ιδιωτικό), consortium blockchain (κοινοπραξιακό) (Buterin, V. (2015)) και hybrid blockchain (υβριδικό). Ας αναλύσουμε όμως το καθένα χωριστά.

Public Blockchain

Το δημόσιο blockchain δεν ανήκει σε κανέναν συγκεκριμένο φορέα, είναι σχεδιασμένο για να είναι πλήρως ανοιχτό και υποστηρίζει την αρχή της αποκέντρωσης, επιτρέποντας σε οποιονδήποτε με υπολογιστή και πρόσβαση στο διαδίκτυο να συμμετάσχει στο δίκτυο χωρίς περιορισμούς. Επιπλέον, κάθε υπολογιστής στο δίκτυο διατηρεί ένα αντίγραφο όλων των άλλων κόμβων ή μπλοκ που περιλαμβάνονται στο σύστημα, ενώ παρέχεται και η δυνατότητα επαλήθευσης συναλλαγών και εγγραφών μέσα στο δίκτυο.

Με την ασφάλεια που παρέχει, μπορεί να αντικαταστήσει τα παραδοσιακά χρηματοοικονομικά συστήματα. Επιπλέον, τα έξυπνα συμβόλαια, τα οποία επιτρέπουν στους χρήστες να πραγματοποιούν αξιόπιστες συναλλαγές χωρίς την ανάγκη για τρίτο μεσάζοντα, ενισχύουν την αποκέντρωση, με παραδείγματα όπως τα Bitcoin και Ethereum να είναι χαρακτηριστικά αυτής της τεχνολογίας. Παρακάτω δίνονται μερικά από τα πλεονεκτήματα και μειονεκτήματά του:

Πλεονεκτήματα

- Ασφάλεια: Το μεγάλο μέγεθος του δημόσιου blockchain, διασφαλίζει μεγαλύτερη διασπορά των εγγραφών.
- Αξιοπιστία: Αλγόριθμοι εντοπίζουν την απάτη, μειώνοντας έτσι τις ανησυχίες των συμμετεχόντων για τους άλλους κόμβους στο δίκτυο.
- Ανωνυμία: Παρέχει μια ασφαλή πλατφόρμα για συναλλαγές, χωρίς να απαιτείται η αποκάλυψη του ονόματος ή της ταυτότητας του χρήστη.
- Αποκέντρωση: Κανένας μεμονωμένος φορέας δεν διαχειρίζεται το δίκτυο, καθώς κάθε χρήστης διαθέτει ένα αντίγραφο του καθολικού.

Μειονεκτήματα

- Ταχύτητα: Εξαιτίας του μεγάλου μεγέθους του, η διαδικασία των συναλλαγών είναι αργή και η επαλήθευση κάθε κόμβου απαιτεί πολύ χρόνο.
- Κατανάλωση Ενέργειας: Καταναλώνει πολύ ενέργεια και απαιτεί ισχυρό υπολογιστικό εξοπλισμό.
- Ρυθμιστικά εμπόδια: Χωρίς κεντρική αρχή, οι κυβερνήσεις αντιμετωπίζουν προβλήματα στην ταχύτερη εφαρμογή της τεχνολογίας.

Private Blockchain

Το ιδιωτικό blockchain δεν είναι τόσο ανοιχτό όσο το δημόσιο, καθώς είναι προσβάσιμο μόνο σε συγκεκριμένους εξουσιοδοτημένους χρήστες. Λειτουργεί σε ένα κλειστό δίκτυο, όπου η συμμετοχή περιορίζεται σε λίγα άτομα, συνήθως εντός μιας εταιρείας ή οργανισμού. Ωστόσο, με την κατάλληλη ασφάλεια και συντήρηση, γίνεται ένα ανεκτίμητο εργαλείο για την προστασία των δεδομένων, χωρίς να εκτίθενται στο ευρύ κοινό. Γι' αυτόν τον λόγο, πολλές εταιρείες το χρησιμοποιούν για εσωτερικούς ελέγχους, ψηφοφορίες και διαχείριση περιουσιακών στοιχείων. Χαρακτηριστικό παράδειγμα ιδιωτικού blockchain είναι το Corda. Ας δούμε ορισμένα από τα πλεονεκτήματα και μειονεκτήματά του:

Πλεονεκτήματα

- Ταχύτητα: Λόγω του μικρού μεγέθους του, η διαδικασία των συναλλαγών είναι γρήγορη και η επαλήθευση κάθε κόμβου απαιτεί λιγότερο χρόνο.
- Ιδιωτικότητα: Το επίπεδο ιδιωτικότητας έχει ενισχυθεί για να καλύψει τις ανάγκες εμπιστευτικότητας των επιχειρήσεων.
- Επεκτασιμότητα: Η επεκτασιμότητα μπορεί να προσαρμοστεί, επιτρέποντας τον χειροκίνητο καθορισμό του μεγέθους του δικτύου.
- Ισορροπία: Υπάρχει καλύτερη ισορροπία, καθώς μόνο συγκεκριμένοι χρήστες έχουν πρόσβαση στις συναλλαγές, γεγονός που βελτιώνει την αποδοτικότητά του.

Μειονεκτήματα

- Ασφάλεια: Είναι πιο ευάλωτο, καθώς ο αριθμός των κόμβων είναι περιορισμένος. Επομένως, μπορεί πιο εύκολα να χειραγωγηθεί.
- Κεντρικοποίηση: Λόγω της κεντρικής φύσης του, ένα από τα κύρια μειονεκτήματα είναι η δυσκολία στη δημιουργία εμπιστοσύνης, καθώς οι οργανισμοί μπορούν να το χρησιμοποιήσουν για αθέμιτες πρακτικές.
- Κόμβοι: Ο μικρός αριθμός κόμβων σημαίνει ότι αν κάποιοι από αυτούς σταματήσουν να λειτουργούν, το σύστημα blockchain μπορεί να τεθεί σε σοβαρό κίνδυνο.

Hybrid Blockchain

Ένα υβριδικό blockchain αποτελεί έναν συνδυασμό ιδιωτικού και δημόσιου blockchain, όπου ένα μέρος του δικτύου ελέγχεται από έναν οργανισμό, ενώ άλλα τμήματα είναι ανοιχτά στο κοινό. Σε αυτό το πλαίσιο, χρησιμοποιούνται τόσο συστήματα που απαιτούν άδεια πρόσβασης όσο και συστήματα χωρίς άδεια. Επιπλέον, οι χρήστες αποκτούν πρόσβαση στις πληροφορίες μέσω έξυπνων συμβολαίων. Τέλος, ακόμα κι αν το υβριδικό blockchain ανήκει σε μια κεντρική οντότητα, δεν επιτρέπεται η τροποποίηση των συναλλαγών.

Αποτελεί μια εξαιρετική λύση για τον τομέα της υγείας, την κυβέρνηση, τα ακίνητα και τις χρηματοοικονομικές εταιρείες. Προσφέρει τη δυνατότητα δημόσιας πρόσβασης στα δεδομένα,

ενώ παράλληλα προστατεύονται ιδιωτικά. Χαρακτηριστικό παράδειγμα υβριδικού blockchain είναι το Ripple (XRP). Μερικά από τα πλεονεκτήματα και μειονεκτήματά του είναι:

Πλεονεκτήματα

- Ασφάλεια: Δεν μπορεί να παραβιαστεί, καθώς το 51% των χρηστών δεν έχει πρόσβαση στο δίκτυο.
- Κόστος: Οι συναλλαγές έχουν χαμηλό κόστος, επειδή μόνο μερικοί κόμβοι συμμετέχουν στην επαλήθευση, μειώνοντας έτσι το υπολογιστικό κόστος.
- Αρχιτεκτονική: Είναι εξαιρετικά προσαρμόσιμο και διατηρεί την ακεραιότητα, την ασφάλεια και τη διαφάνεια.
- Διαχείριση: Μπορεί να επιλέξει τους συμμετέχοντες στο blockchain και να αποφασίσει ποιες συναλλαγές θα είναι δημόσιες.

Μειονεκτήματα

- Ασφάλεια: Εξαιτίας του κλειστού χαρακτήρα του, δεν υπάρχουν αρκετά κίνητρα για συμμετοχή στο δίκτυο.
- Αποδοτικότητα: Η εφαρμογή του δεν είναι εφικτή για όλους, και οι οργανισμοί συχνά αντιμετωπίζουν δυσκολίες στη διατήρηση της αποδοτικότητάς του.
- Διαφάνεια: Υπάρχει η δυνατότητα να αποκρυφτούν πληροφορίες από τον χρήστη. Η πρόσβαση σε ένα υβριδικό blockchain εξαρτάται από την απόφαση του οργανισμού, ο οποίος μπορεί να επιλέξει αν θα την επιτρέψει ή όχι.

Consortium Blockchain

Το κοινοπραξιακό blockchain αποτελεί μια καινοτόμο λύση που ανταποκρίνεται στις απαιτήσεις των οργανισμών. Αυτή η τεχνολογία όχι μόνο επικυρώνει τις συναλλαγές, αλλά μπορεί επίσης να τις ξεκινήσει ή να τις δεχτεί. Ένα μέρος του δικτύου είναι ανοιχτό στο κοινό, ενώ άλλο μέρος παραμένει ιδιωτικό, και η διαχείρισή του γίνεται από πολλούς οργανισμούς. Παράλληλα, έχει υψηλές δυνατότητες σε επιχειρήσεις, τράπεζες και άλλους φορείς επεξεργασίας πληρωμών. Χαρακτηριστικό παράδειγμα κοινοπραξιακού blockchain είναι το Tendermint. Παρακάτω δίνονται κάποια από τα πλεονεκτήματα και μειονεκτήματά του:

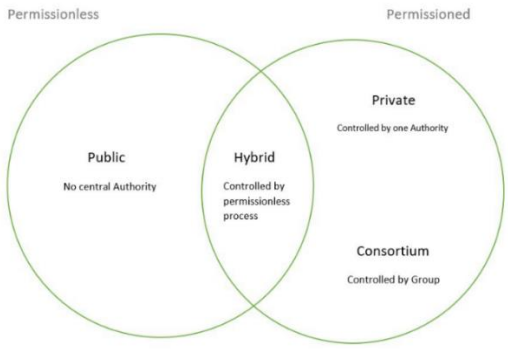
Πλεονεκτήματα

- Ταχύτητα: Η περιορισμένη συμμετοχή χρηστών επιτρέπει γρήγορη επαλήθευση, καθιστώντας το σύστημα πιο αποδοτικό για τους οργανισμούς.
- Ιδιωτικότητα: Οι πληροφορίες του παραμένουν κρυφές από το κοινό, αλλά οποιοδήποτε μέλος του μπορεί να τις δει.
- Αποκέντρωση: Πολλοί οργανισμοί μπορούν να συμμετέχουν, επιτυγχάνοντας αποκέντρωση σε όλα τα επίπεδα, αυξάνοντας έτσι την ασφάλεια του συστήματος.
- Ευελιξία: Οι αποφάσεις μπορούν να ληφθούν πιο γρήγορα, καθώς δεν είναι πολύ εκτεταμένο.

Μειονεκτήματα

- Ασφάλεια: Αν παραβιαστούν κάποιοι κόμβοι, υπάρχει αυξημένος κίνδυνος για αδυναμία ασφάλειας σε αυτό το blockchain.
- Διαφάνεια: Υπάρχει πιθανότητα παραβίασης εάν ο οργανισμός διαφθαρεί. Οι οργανισμοί ενδέχεται να κρύψουν πληροφορίες από τους χρήστες.
- Έγκριση: Η έγκριση του πρωτοκόλλου από όλα τα μέλη μειώνει την ευελιξία του. Καθώς συμμετέχουν ένας ή περισσότεροι οργανισμοί, μπορεί να προκύψουν διαφορές στις απόψεις ή στα συμφέροντα.

Το Blockchain Overlay Network είναι υπεύθυνο για τον συγχρονισμό των διαφορετικών τύπων blockchains και τη διαχείριση των λειτουργιών τους (Priyadarshini, I. (2019)).



Εικόνα 1. Οι διάφοροι τύποι blockchain.

2.1.2. Μηχανισμοί Συναίνεσης

Ο μηχανισμός συναίνεσης, εντός της τεχνολογίας Blockchain, αποτελεί ένα κρίσιμο πρωτόκολλο που εξασφαλίζει τη συμφωνία όλων των κόμβων, δηλαδή των υπολογιστών που συμμετέχουν σε ένα δίκτυο blockchain, σχετικά με την τρέχουσα κατάσταση του κατανεμημένου καθολικού. Με άλλα λόγια, πρόκειται για μια διαδικασία επίτευξης συμφωνίας σε ένα κατανεμημένο σύστημα, η οποία επιτρέπει στο δίκτυο να επιβεβαιώνει συναλλαγές και να αποτρέπει το φαινόμενο της επαναλαμβανόμενης δαπάνης χωρίς την ανάγκη ύπαρξης κεντρικής αρχής. Επιπλέον, ο μηχανισμός συναίνεσης στοχεύει στην επικύρωση και την επαλήθευση των συναλλαγών, διασφαλίζοντας παράλληλα την ακεραιότητα και την ασφάλεια του blockchain. Μέσω αυτής της διαδικασίας, εξασφαλίζεται ότι όλοι οι κόμβοι διαθέτουν την ίδια έκδοση του καθολικού του blockchain.

Διάφορα δίκτυα blockchain χρησιμοποιούν διαφορετικούς μηχανισμούς συναίνεσης, καθένας από τους οποίους έχει τα δικά του πλεονεκτήματα και μειονεκτήματα. Ορισμένοι από τους πιο κοινά χρησιμοποιούμενους μηχανισμούς συναίνεσης περιλαμβάνουν το Proof of Work (PoW), το Proof of Stake (PoS), το Delegated Proof of Stake (DPoS), και το Byzantine Fault Tolerance (BFT), μεταξύ άλλων.

Αξίζει να σημειωθεί ότι οι μηχανισμοί αυτοί διαδραματίζουν καθοριστικό ρόλο στην ανθεκτικότητα της τεχνολογίας blockchain απέναντι στις επιθέσεις Sybil. Σε τέτοιες επιθέσεις, ένας κακόβουλος παράγοντας θα μπορούσε να δημιουργήσει πολλαπλές ψευδοανώνυμες ταυτότητες, με σκοπό να αποκτήσει δυσανάλογα μεγάλη επιρροή στο δίκτυο.

Στη συνέχεια, αναλύονται οι 10 πιο κοινοί μηχανισμοί συναίνεσης:

1. Proof of Work (PoW)

Το PoW είναι ένας μηχανισμός συναίνεσης που χρησιμοποιείται κυρίως στο δίκτυο του Bitcoin, αλλά και στο Ethereum (Nakamoto, S (2008)). Σε ένα αποκεντρωμένο δίκτυο, είναι απαραίτητο να επιλεγεί κάποιος κόμβος για να καταγράψει τις συναλλαγές, και ενώ η τυχαία επιλογή θα ήταν η πιο απλή μέθοδος, είναι ευάλωτη σε επιθέσεις. Γι' αυτόν τον λόγο, στο PoW απαιτείται να γίνει μια σημαντική υπολογιστική εργασία από τους κόμβους, προκειμένου να αποδείξουν ότι δεν σκοπεύουν να επιτεθούν στο δίκτυο. Αυτή η εργασία περιλαμβάνει τον υπολογισμό μιας τιμής hash του μπλοκ κεφαλίδας (block header), η οποία περιέχει ένα nonce (αριθμός ή τιμή που μπορεί να χρησιμοποιηθεί μόνο μια φορά). Οι κόμβοι που υπολογίζουν τις τιμές hash ονομάζονται εξορύκτες και η διαδικασία PoW ονομάζεται εξόρυξη στο Bitcoin.

Οι εξορύκτες αλλάζουν συχνά το nonce για να επιτύχουν διαφορετικές τιμές hash, με στόχο να βρουν μια τιμή που να πληροί συγκεκριμένα κριτήρια, δηλαδή να είναι ίση ή μικρότερη από μια καθορισμένη τιμή. Όταν ένας κόμβος πετύχει αυτήν την τιμή, μεταδίδει το νέο μπλοκ στους υπόλοιπους κόμβους του δικτύου, οι οποίοι πρέπει να επιβεβαιώσουν την ορθότητα της τιμής hash. Εφόσον το μπλοκ επικυρωθεί, οι άλλοι εξορύκτες το προσθέτουν στις αλυσίδες τους. Στην περίπτωση που δύο κόμβοι βρουν ταυτόχρονα τον κατάλληλο αριθμό nonce και δημιουργηθούν έγκυρα μπλοκ, ενδέχεται να σχηματιστούν διακλαδώσεις. Αλλά, είναι απίθανο δύο ανταγωνιστικές διακλαδώσεις να δημιουργήσουν το επόμενο μπλοκ ταυτόχρονα. Ωστόσο, στο PoW, η μεγαλύτερη αλυσίδα είναι γνωστή ως "αυθεντική" και οι εξορύκτες συνεχίζουν να εργάζονται πάνω σε αυτήν.

Αν και το PoW προσφέρει αποκέντρωση και ασφάλεια, έχει σημαντικά μειονεκτήματα, όπως η υψηλή υπολογιστική απαίτηση και η υπερβολική κατανάλωση ενέργειας. Επιπλέον, είναι ευάλωτο σε επιθέσεις 51%, όπου ένας κακόβουλος παράγοντας θα μπορούσε να αποκτήσει τον έλεγχο της πλειονότητας του δικτύου. Για να μετριαστεί η σπατάλη πόρων, έχουν αναπτυχθεί εναλλακτικά πρωτόκολλα PoW με παράπλευρες εφαρμογές, όπως το Primecoin (King, S. (2013)), το οποίο αναζητά ειδικές ακολουθίες πρώτων αριθμών που μπορούν να χρησιμοποιηθούν στη μαθηματική έρευνα.

2. Proof of Stake (PoS)

Το PoS αποτελεί μια ενεργειακά αποδοτική εναλλακτική λύση σε σχέση με το PoW. Σε αντίθεση με το PoW, όπου οι εξορύκτες πρέπει να λύσουν πολύπλοκους μαθηματικούς γρίφους, στο PoS οι επικυρωτές αποδεικνύουν την ιδιοκτησία ενός συγκεκριμένου ποσού κρυπτονομισμάτων, γνωστό ως "stake". Αυτή η προσέγγιση βασίζεται στην υπόθεση ότι τα άτομα με μεγαλύτερο stake έχουν μικρότερο κίνητρο να επιτεθούν στο δίκτυο, καθώς διακυβεύεται το ίδιο τους το κεφάλαιο. Ωστόσο, η απλή επιλογή με βάση το υπόλοιπο του λογαριασμού μπορεί να θεωρηθεί άδικη, καθώς τα άτομα με τα περισσότερα κρυπτονομίσματα θα κυριαρχούσαν στο δίκτυο.

Για την αντιμετώπιση αυτής της ανισότητας, έχουν προταθεί διάφορες λύσεις που συνδυάζουν το μέγεθος του μεριδίου με άλλες παραμέτρους για τον καθορισμό του ποιος θα δημιουργήσει το επόμενο μπλοκ. Για παράδειγμα, το Blackcoin (Vasin, P. (2014)) χρησιμοποιεί τυχαία επιλογή σε συνδυασμό με τη χαμηλότερη τιμή hash και το μέγεθος του μεριδίου, ενώ το Peercoin (King, S. and Nadal, S. (2012)) προτιμά την επιλογή με βάση την ηλικία των νομισμάτων, δίνοντας μεγαλύτερη πιθανότητα εξόρυξης του επόμενου μπλοκ σε παλαιότερα και μεγαλύτερα σύνολα νομισμάτων.

Σε σύγκριση με το PoW, το PoS είναι πιο ενεργειακά αποδοτικό και γενικότερα πιο αποτελεσματικό, καθώς δεν απαιτεί τους ίδιους υπερβολικούς υπολογιστικούς πόρους. Ωστόσο, η σχεδόν μηδενική ανάγκη για υπολογιστική ισχύ μπορεί να οδηγήσει σε αυξημένο κίνδυνο επιθέσεων. Παρόλα αυτά, πολλά blockchains, όπως το Ethereum 2.0 και το Cardano, έχουν υιοθετήσει το PoS, με σκοπό να επωφεληθούν από τα πλεονεκτήματα του.

3. Delegated Proof of Stake (DPoS)

Το DPoS είναι ένας καινοτόμος μηχανισμός συναίνεσης που διαφέρει από το παραδοσιακό PoS, κυρίως ως προς τον τρόπο διακυβέρνησης και διαχείρισης του δικτύου. Στο πλαίσιο του DPoS, οι κάτοχοι νομισμάτων εκλέγουν αντιπροσώπους για να αναλαμβάνουν τη δημιουργία και επικύρωση μπλοκ. Αυτή η διαδικασία ενσωματώνει έναν μικρότερο αριθμό επικυρωτών σε σύγκριση με το PoS, γεγονός που επιτρέπει την ταχύτερη επιβεβαίωση των συναλλαγών.

Οι αντιπρόσωποι που εκλέγονται έχουν την ευθύνη για την επικύρωση των μπλοκ και τη διατήρηση του blockchain, ενώ οι παράμετροι του δικτύου, όπως το μέγεθος των μπλοκ και τα διαστήματα μεταξύ τους, μπορούν να ρυθμιστούν από αυτούς. Αυτή η ρύθμιση δημιουργεί ένα πιο ευέλικτο και δημοκρατικό σύστημα διακυβέρνησης, καθώς οι χρήστες έχουν τη δυνατότητα να απομακρύνουν ανέντιμους αντιπροσώπους μέσω ψηφοφορίας, διασφαλίζοντας τη διαφάνεια και την αξιοπιστία του δικτύου.

Επιπλέον, το DPoS είναι γνωστό για την ταχύτητα στην επιβεβαίωση συναλλαγών και την ενεργειακή του αποδοτικότητα. Παρόλο που προσφέρει αυτά τα πλεονεκτήματα, ενδέχεται να υπάρξει κίνδυνος κεντροποίησης λόγω του περιορισμένου αριθμού επικυρωτών. Παρά τις προκλήσεις αυτές, το DPoS στοχεύει στο να δημιουργήσει ένα πιο αποδοτικό και δημοκρατικό σύστημα, το οποίο υιοθετείται από blockchains όπως το Tron και το EOS.

4. Leased Proof of Stake (LPoS)

Το LPoS χρησιμοποιείται από το blockchain του Waves και αποτελεί έναν καινοτόμο τρόπο διασφάλισης της αξιοπιστίας και της ασφάλειας του δικτύου. Μέσω του LPoS, οι κάτοχοι tokens έχουν τη δυνατότητα να ενοικιάζουν το υπόλοιπό τους σε πλήρεις κόμβους, προσφέροντάς τους αυξημένη «ισχύ στοιχήματος». Αυτό σημαίνει ότι οι πλήρεις κόμβοι γίνονται πιο πιθανό να επικυρώσουν συναλλαγές και να προσθέσουν νέα μπλοκ στο blockchain. Σε αντάλλαγμα, οι κάτοχοι των tokens λαμβάνουν ένα μέρος από τα τέλη συναλλαγών ως ανταμοιβή, προσφέροντας μια ευκαιρία για παθητικό εισόδημα. Αυτό το σύστημα όχι μόνο ενισχύει την ασφάλεια του δικτύου, αλλά και ενθαρρύνει τη συμμετοχή των χρηστών, καθιστώντας το ένα σημαντικό εργαλείο για τη διατήρηση της ακεραιότητας του δικτύου.

5. Proof of Authority (PoA)

Το PoA αποτελεί έναν μηχανισμό συναίνεσης που εφαρμόζεται κυρίως σε αδειοδοτημένα blockchains, όπως το VeChain. Σε αυτό το σύστημα, οι συναλλαγές και τα blocks επικυρώνονται από προκαθορισμένους λογαριασμούς, τους επικυρωτές, οι οποίοι είναι αξιόπιστα άτομα ή οντότητες με επαληθευμένες ταυτότητες. Αυτή η διασφάλιση ταυτότητας προσφέρει αξιοπιστία και υπευθυνότητα στο δίκτυο.

Η PoA χαρακτηρίζεται από την υψηλή ταχύτητα συναλλαγών, την ενεργειακή αποδοτικότητα και την απαίτηση για την καλή φήμη των επικυρωτών, καθιστώντας την ιδανική για αδειοδοτημένα blockchains. Αυτά τα χαρακτηριστικά συνδυάζονται για να δημιουργήσουν ένα αποτελεσματικό και αξιόπιστο σύστημα συναίνεσης, κατάλληλο για εφαρμογές που απαιτούν υψηλά επίπεδα ασφαλείας και διαφάνειας.

6. Byzantine Fault Tolerance (BFT)

Το BFT αποτελεί έναν σημαντικό μηχανισμό συναίνεσης που εφαρμόζεται σε blockchains, όπως το Hyperledger. Σχεδιάστηκε για να προστατεύει τα κατανεμημένα συστήματα από διάφορες πιθανές αποτυχίες και κακόβουλες ενέργειες. Με τον μηχανισμό BFT, ένα σύστημα μπορεί να συνεχίσει να λειτουργεί σωστά και να επιτυγχάνει συναίνεση, υπό την προϋπόθεση ότι ο αριθμός των προδοτικών κόμβων δεν υπερβαίνει ένα καθορισμένο όριο, εξασφαλίζοντας έτσι την ανθεκτικότητα και την ασφάλεια του δικτύου.

Αυτός ο μηχανισμός διακρίνεται για την υψηλή ανοχή του σε σφάλματα, καθώς και την ικανότητά του να μετριάζει τις κακόβουλες ενέργειες. Επιπλέον, η διαδικασία λήψης αποφάσεων είναι γρήγορη, ενώ ταυτόχρονα απαιτείται εμπιστοσύνη στους επικυρωτές για την ομαλή λειτουργία του συστήματος. Συνολικά, ο BFT προσφέρει μια αξιόπιστη και αποτελεσματική λύση για τη διατήρηση της ακεραιότητας και της σταθερότητας στα κατανεμημένα δίκτυα.

7. Proof of Space (PoSpace)

Το PoSpace, γνωστό και ως Απόδειξη Χωρητικότητας, αποτελεί έναν καινοτόμο μηχανισμό συναίνεσης που εφαρμόζεται σε blockchains όπως το Chia. Σε αυτό το πλαίσιο, οι miners δεσμεύουν χώρο στον δίσκο τους για να επιλύσουν υπολογιστικές προκλήσεις. Όσο μεγαλύτερη αποθηκευτική χωρητικότητα δεσμεύει ένας miner, τόσο αυξάνονται οι πιθανότητές του να προσθέσει ένα νέο block στην αλυσίδα. Αυτός ο μηχανισμός ξεχωρίζει, καθώς είναι πιο ενεργειακά αποδοτικός σε σύγκριση με άλλους, όπως το PoW. Επιπλέον, η χρήση αποθηκευτικού χώρου ως πόρου όχι μόνο μειώνει την ενεργειακή κατανάλωση, αλλά απαιτεί επίσης σημαντική χωρητικότητα αποθήκευσης, γεγονός που συμβάλλει στην αποφυγή συγκεντρωτισμού, προσφέροντας μεγαλύτερη ασφάλεια και αποκέντρωση στο δίκτυο.

8. Proof of Burn (PoB)

Το PoB αποτελεί έναν ιδιαίτερο μηχανισμό συναίνεσης που χρησιμοποιείται από blockchains, όπως το Slimcoin. Στο πλαίσιο του PoB, οι miners συμμετέχουν στη διαδικασία συναίνεσης «καίγοντας» ένα μέρος των νομισμάτων τους, δηλαδή αφαιρώντας τα οριστικά από την κυκλοφορία, μέσω της αποστολής τους σε μη διαθέσιμες διευθύνσεις. Αυτό τους παρέχει το δικαίωμα να δημιουργούν νέα blocks, με την πιθανότητα επιτυχίας να εξαρτάται από τον αριθμό των νομισμάτων που έχουν κάψει.

Με την πάροδο του χρόνου, ο μηχανισμός αυτός αναδεικνύεται ως πιο ενεργειακά αποδοτικός συγκριτικά με άλλους μηχανισμούς όπως το PoW, καθώς δεν απαιτεί την κατανάλωση μεγάλης ποσότητας ηλεκτρικής ενέργειας. Επιπλέον, το PoB ενθαρρύνει τη μακροπρόθεσμη δέσμευση των συμμετεχόντων, καθώς η διαδικασία του «καψίματος» των νομισμάτων τους συνδέεται με τη διαρκή δέσμευση στο δίκτυο.

Τέλος, συμβάλλει στη μείωση των επιθέσεων εγωιστικής εξόρυξης, καθώς η διαδικασία καύσης καθιστά τέτοιου είδους επιθέσεις λιγότερο επωφελείς, ενισχύοντας έτσι την ασφάλεια και τη σταθερότητα του δικτύου.

9. Proof of Importance (PoI)

Το PoI είναι ένας καινοτόμος μηχανισμός συναίνεσης που χρησιμοποιείται από το blockchain NEM. Σε αντίθεση με το PoS, όπου η συμμετοχή καθορίζεται κυρίως από τον αριθμό των κατεχόμενων tokens, το PoI αξιολογεί την ουσιαστική υποστήριξη που προσφέρει κάθε χρήστης στο δίκτυο. Συγκεκριμένα, λαμβάνονται υπόψη όχι μόνο η ποσότητα των tokens που κατέχει ο χρήστης, αλλά και η συμπεριφορά του στις συναλλαγές, συμπεριλαμβανομένου του αριθμού των συναλλαγών και της φύσης των αλληλεπιδράσεων με άλλους χρήστες. Αυτή η πολυδιάστατη προσέγγιση επιτρέπει στο PoI να ανταμείβει τη συνολική συνεισφορά προς το δίκτυο, καθιστώντας τον μηχανισμό πιο δίκαιο και αντιπροσωπευτικό σε σύγκριση με το PoS.

Με αυτόν τον τρόπο, το PoI ενθαρρύνει την ενεργή συμμετοχή στο δίκτυο, δίνοντας έμφαση όχι μόνο στην κατοχή, αλλά και στην πραγματική χρήση και υποστήριξη του συστήματος. Αυτή η

διαφοροποίηση ενισχύει την ισορροπία και τη δικαιοσύνη στο σύστημα, προάγοντας ένα πιο δυναμικό και συμμετοχικό περιβάλλον για όλους τους χρήστες του δικτύου.

10. Proof of History (PoH)

Το PoH είναι ένας αλγόριθμος συναίνεσης που χρησιμοποιείται από το blockchain Solana, ο οποίος εισάγει μια επαληθεύσιμη χρονική σήμανση στις συναλλαγές. Αυτή η καινοτόμος προσέγγιση δημιουργεί ένα ιστορικό αρχείο που επιβεβαιώνει ότι ένα γεγονός έλαβε χώρα σε μια συγκεκριμένη χρονική στιγμή. Χάρη σε αυτόν τον μηχανισμό, επιτυγχάνεται σημαντική αύξηση στην κλιμάκωση και την ταχύτητα των συναλλαγών. Επιπλέον, η χρήση του PoH βελτιώνει τη συνολική αποδοτικότητα του δικτύου, καθιστώντας το πιο αποτελεσματικό και ταχύ στη διαχείριση των συναλλαγών.

Συνοψίζοντας, οι μηχανισμοί συναίνεσης είναι θεμελιώδεις για τη λειτουργία της τεχνολογίας Blockchain, καθώς της επιτρέπουν να παραμένει αποκεντρωμένη, διαφανής και ασφαλής, προσφέροντας ταυτόχρονα μια αξιόπιστη και ανθεκτική πλατφόρμα συναλλαγών.

2.2. Δομή και Λειτουργία

Η τεχνολογία Blockchain λειτουργεί ως ένα κατανεμημένο αρχείο βάσης δεδομένων ή ως ένα δημόσιο καθολικό, στο οποίο όλες οι συναλλαγές που έχουν πραγματοποιηθεί αποθηκεύονται σε μια λίστα από μπλοκ, που συνεχώς μεγαλώνει καθώς προστίθενται νέα μπλοκ (Zheng, Z. et al. (2017)). Αυτές οι συναλλαγές ή διαδικασίες εκτελούνται ψηφιακά και μοιράζονται μεταξύ των συμμετεχόντων. Εδώ να τονίσουμε ότι, κάθε συναλλαγή που καταγράφεται επικυρώνεται μέσω της κοινής συμφωνίας όλων των εμπλεκόμενων μερών και μόλις εισαχθεί στο σύστημα, δεν μπορεί ποτέ να διαγραφεί. Η τεχνολογία Blockchain επιτρέπει την εύκολη επαλήθευση και καταγραφή κάθε συναλλαγής που πραγματοποιείται εντός του συστήματος (Singh, G., Garg, V. & Tiwari, P. (2021)).

Αρχικά, θα δούμε ποια είναι τα βασικά στοιχεία της δομής της τεχνολογίας Blockchain:

-**Κόμβος**: Χρήστης ή υπολογιστής στη δομή του blockchain, όπου κάθε κόμβος διαθέτει ένα ανεξάρτητο αντίγραφο του συνολικού καθολικού του blockchain.

-**Συναλλαγή:** Το μικρότερο δομικό στοιχείο ενός συστήματος blockchain, όπως αρχεία, πληροφορίες, που εξυπηρετεί τον σκοπό του blockchain. Μπορεί να δημιουργούνται από πελάτες ή εφαρμογές πελατών (Priyadarshini, I. (2019)).

-**Μπλοκ**: Δομή δεδομένων που αποθηκεύει ένα σύνολο συναλλαγών και διανέμεται σε όλους τους κόμβους του δικτύου. Το πρώτο μπλοκ ενός blockchain ονομάζεται "genesis" μπλοκ (Zheng, Z. et al. (2017)).

-**Αλυσίδα**: Ακολουθία μπλοκ τοποθετημένα σε συγκεκριμένη σειρά.

-**Εξορύκτες (miners)**: Συγκεκριμένοι κόμβοι που πραγματοποιούν τη διαδικασία επαλήθευσης μπλοκ πριν προσθέσουν οτιδήποτε στη δομή του blockchain.

-Συναίνεση (πρωτόκολλο συναίνεσης): Σύνολο κανόνων και συμφωνιών που καθοδηγούν την εκτέλεση των λειτουργιών του blockchain.

Στη συνέχεια, είναι σημαντικό να εξετάσουμε τα πέντε βασικά επίπεδα της δομής του blockchain, προκειμένου να κατανοήσουμε καλύτερα τη λειτουργία και τις δυνατότητές αυτής της τεχνολογίας.

The Hardware Layer

Τα δεδομένα ενός blockchain μπορούν να αποθηκευτούν τόσο σε μεμονωμένους κόμβους όσο και σε έναν διακομιστή σε ένα κέντρο δεδομένων. Συνήθως, όταν οι χρήστες πλοηγούνται στο διαδίκτυο ή χρησιμοποιούν εφαρμογές, βασίζονται σε μια αρχιτεκτονική πελάτη-διακομιστή για να ζητήσουν και να λάβουν δεδομένα από διακομιστές εφαρμογών. Σε αυτό το πλαίσιο, οι πελάτες έχουν τη δυνατότητα να επικοινωνούν απευθείας μεταξύ τους και να ανταλλάσσουν δεδομένα. Ένα τέτοιο δίκτυο, όπου οι υπολογιστές μοιράζονται δεδομένα μεταξύ τους, είναι γνωστό ως ομότιμο δίκτυο (peer-to-peer – P2P). Ως εκ τούτου, όλες οι πληροφορίες, συμπεριλαμβανομένων των δεδομένων και των συναλλαγών, αποθηκεύονται σε μια κατανεμημένη βάση δεδομένων, διασφαλίζοντας έτσι την ακεραιότητα και την αποκεντρωμένη φύση του συστήματος.

The Data Layer

Η δομή δεδομένων ενός blockchain μπορεί να περιγραφεί ως μια οργανωμένη αλυσίδα μπλοκ. Τα δύο βασικά στοιχεία της είναι οι δείκτες και η συνδεδεμένη λίστα. Οι δείκτες είναι μεταβλητές που υποδεικνύουν τη θέση μιας άλλης μεταβλητής, ενώ η συνδεδεμένη λίστα είναι μια αλυσίδα από μπλοκ που περιλαμβάνουν δεδομένα και δείκτες προς το προηγούμενο μπλοκ. Οι συναλλαγές υπογράφονται ψηφιακά για να εξασφαλιστεί η ασφάλεια και η ακεραιότητα των δεδομένων που βρίσκονται στα διάφορα επίπεδα του συστήματος. Αυτή η διαδικασία βασίζεται στη χρήση δύο κρυπτογραφικών κλειδιών που αλληλοεπαληθεύονται, ενός δημόσιου και ενός ιδιωτικού (Aggarwal, S. and Kumar, N. (2021)), όπου ο υπογράφων μπορεί να επαληθευτεί από

οποιονδήποτε διαθέτει το αντίστοιχο δημόσιο κλειδί. Με αυτόν τον τρόπο, διασφαλίζεται τόσο η ακεραιότητα όσο και η προστασία των πληροφοριών από τυχόν τροποποιήσεις, καθώς τα δεδομένα κρυπτογραφούνται με ένα μοναδικό hash που δεν μπορεί να αλλοιωθεί. Επιπλέον, η ταυτότητα του αποστολέα ή του ιδιοκτήτη παραμένει προστατευμένη και δεν είναι άμεσα ανιχνεύσιμη, καθιστώντας την υπογραφή αμετάκλητα συνδεδεμένη με τον κάτοχό της. Ο αλγόριθμος ψηφιακής υπογραφής που χρησιμοποιείται συνήθως στα blockchains είναι ο αλγόριθμος ψηφιακής υπογραφής με ελλειπτική καμπύλη (Elliptic Curve Digital Signature Algorithm, ECDSA) (Nalayini, C. M. et al. (2023)).

The Network Layer

Το επίπεδο δικτύου αποτελεί το σημείο όπου πραγματοποιείται η επικοινωνία μεταξύ των κόμβων, οι οποίοι μοιράζονται τα φορτία του δικτύου για να επιτύχουν έναν κοινό στόχο. Είναι γνωστό και ως επίπεδο P2P ή επίπεδο διάδοσης. Σε αυτό το επίπεδο, διαχειρίζεται η διάδοση των μπλοκ και των συναλλαγών. Επιπλέον, εξασφαλίζεται η δυνατότητα σύνδεσης, επικοινωνίας, ανταλλαγής δεδομένων και συγχρονισμού των κόμβων, διατηρώντας έτσι την ακεραιότητα του δικτύου. Τέλος, οι κόμβοι είναι υπεύθυνοι για την επεξεργασία των συναλλαγών στο blockchain.

The Consensus Layer

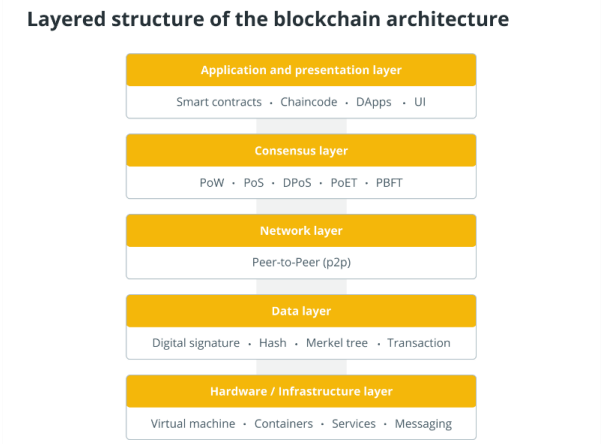
Το επίπεδο συναίνεσης είναι ζωτικής σημασίας για τη λειτουργία των πλατφόρμων blockchain, είτε πρόκειται για Ethereum, είτε για άλλα blockchain συστήματα. Αυτό το επίπεδο διαδραματίζει κεντρικό ρόλο, καθώς είναι υπεύθυνο για την οργάνωση, την επικύρωση και τη διασφάλιση ότι τα μπλοκ ακολουθούν τη σωστή αλληλουχία. Επιπλέον, το επίπεδο συναίνεσης καθιερώνει ένα συγκεκριμένο σύνολο συμφωνιών μεταξύ των κόμβων, με βάση τους οποίους επικυρώνονται οι συναλλαγές, χρησιμοποιώντας την Απλή Επαλήθευση Πληρωμών (SPV) (Priyadarshini, I. (2019)) και δημιουργούνται τα μπλοκ. Είναι σημαντικό να σημειωθεί ότι

κανείς δεν έχει απόλυτο έλεγχο στο blockchain, καθώς το επίπεδο συναίνεσης διατηρεί την εξουσία κατανεμημένη και αποκεντρωμένη.

The Application Layer

Το επίπεδο εφαρμογής φιλοξενεί όλες τις εφαρμογές που συνδέονται με το πρωτόκολλο. Με άλλα λόγια, είναι το σημείο όπου αναπτύσσονται και λειτουργούν όλες οι εφαρμογές στο δίκτυο. Σε αυτό περιλαμβάνονται βασικά στοιχεία, όπως οι αποκεντρωμένες εφαρμογές (dApps), τα έξυπνα συμβόλαια, οι διεπαφές προγραμματισμού εφαρμογών (APIs), οι διεπαφές χρήστη, καθώς και ο κώδικας αλυσίδας (chain code).

Αυτό το επίπεδο όχι μόνο επεκτείνει τη λειτουργικότητα του blockchain πέρα από το απλό κατανεμημένο καθολικό, αλλά παρέχει επίσης στους τελικούς χρήστες προγράμματα που βασίζονται στην τεχνολογία blockchain. Τα προγράμματα αυτά λειτουργούν ως το frontend, επιτρέποντας στους χρήστες να αλληλεπιδρούν με το blockchain, το οποίο δρα ως το backend. Επιπλέον, διασφαλίζει τη ντετερμινιστική φύση του blockchain, εξασφαλίζοντας ότι κάθε εκτελούμενη συναλλαγή παράγει το ίδιο αποτέλεσμα, γεγονός που επιτρέπει στους κόμβους να επιτυγχάνουν συναίνεση.



Εικόνα 2. Τα βασικά επίπεδα της τεχνολογίας Blockchain (Πηγή: InBlog).

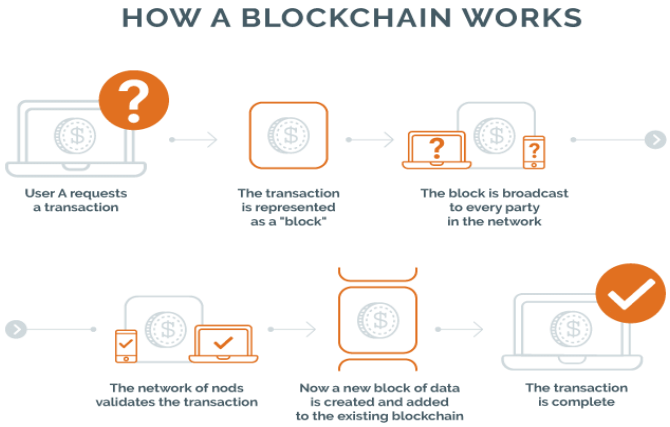
Έπειτα, θα δούμε πώς λειτουργεί η τεχνολογία Blockchain και συγκεκριμένα θα δούμε πώς αυτή εφαρμόζεται στο δημοφιλές παράδειγμα των bitcoins.

Όπως έχουμε ήδη αναφέρει, η τεχνολογία blockchain καταργεί την ανάγκη για τρίτα μέρη στην επικύρωση των συναλλαγών, βασιζόμενη αντ' αυτού σε κρυπτογραφικές αποδείξεις. Επίσης, οι συναλλαγές προστατεύονται μέσω ψηφιακών υπογραφών. Συγκεκριμένα, ο παραλήπτης διαθέτει ένα δημόσιο κλειδί, στο οποίο αποστέλλεται κάθε συναλλαγή, και χρησιμοποιεί το ιδιωτικό κλειδί του αποστολέα για να υπογράψει ψηφιακά τη συναλλαγή. Στη συνέχεια, ο κάτοχος του κρυπτονομίσματος πρέπει να αποδείξει την κατοχή του ιδιωτικού κλειδιού για να μπορέσει να ξοδέψει το νόμισμα. Τέλος, ο παραλήπτης της ψηφιακής συναλλαγής οφείλει να επαληθεύσει την υπογραφή και την κατοχή του ιδιωτικού κλειδιού χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, ώστε η συναλλαγή να θεωρηθεί έγκυρη.
Μόλις ολοκληρωθεί η συναλλαγή, κοινοποιείται σε όλους τους κόμβους του δικτύου Bitcoin, οι οποίοι πρέπει πρώτα να την επαληθεύσουν και στη συνέχεια να την καταγράψουν. Δεδομένου ότι η εγκυρότητα κάθε συναλλαγής είναι απαραίτητη προϋπόθεση πριν από την καταγραφή της στο δημόσιο καθολικό, για να προχωρήσει ένας κόμβος στην καταγραφή της, πρέπει πρώτα να επαληθεύσει δύο στοιχεία (Priyadarshini, I. (2019)): Πρώτον, ότι το κρυπτονόμισμα ανήκει στον χρήστη που το ξοδεύει, κάτι που επιβεβαιώνεται μέσω της ψηφιακής υπογραφής. Δεύτερον, ότι ο χρήστης διαθέτει επαρκές κρυπτονόμισμα για να ολοκληρώσει τη συναλλαγή, το οποίο μπορεί να ελεγχθεί μέσω του ιστορικού των συναλλαγών στον λογαριασμό του (Priyadarshini, I. (2019)).

Σε αυτό το σημείο αξίζει να αναφέρουμε ότι, η τεχνολογία Blockchain αναπτύχθηκε ακριβώς για να δημιουργήσει έναν μηχανισμό που θα εξασφάλιζε τη συμφωνία ολόκληρου του δικτύου στις συναλλαγές Bitcoin. Στα αρχικά στάδια, πριν από την ανάπτυξη της και όταν τα bitcoins ήταν κυρίαρχα, οι συναλλαγές δεν πραγματοποιούνταν πάντα με τη σωστή σειρά, γεγονός που ανέδειξε την ανάγκη να εξαλειφθεί το πρόβλημα της διπλής δαπάνης του κρυπτονομίσματος. Ειδικότερα, οι συναλλαγές μεταφέρονται από κόμβο σε κόμβο μέσα σε ένα δίκτυο bitcoin, με αποτέλεσμα η σειρά που λαμβάνονται οι συναλλαγές σε έναν κόμβο να μην ανταποκρίνεται πάντα στην πραγματική σειρά με την οποία πραγματοποιούνται.

Για παράδειγμα, η Συναλλαγή Α μπορεί να πραγματοποιηθεί πριν από τη Συναλλαγή Β, ωστόσο η Συναλλαγή Α μπορεί να χρειαστεί να περάσει από περισσότερους κόμβους σε σχέση με τη Συναλλαγή Β, με αποτέλεσμα η Συναλλαγή Β να καταγραφεί πρώτη σε έναν συγκεκριμένο κόμβο. Αυτό το πρόβλημα, το Bitcoin κατάφερε να το λύσει με τη χρήση της τεχνολογίας Blockchain. Οι συναλλαγές οργανώθηκαν σε μπλοκ, οδηγώντας έτσι στη δημιουργία των

blockchains. Αυτό σημαίνει ότι όλες οι συναλλαγές που περιλαμβάνονται σε ένα μπλοκ θεωρείται ότι έχουν πραγματοποιηθεί ταυτόχρονα. Στη συνέχεια, τα μπλοκ τοποθετούνται στη σε μια γραμμική, χρονολογική σειρά, έτσι ώστε κάθε μπλοκ να συνδέεται με το προηγούμενο μέσω της τιμής κατακερματισμού του (hash value).



Εικόνα 3. Ο τρόπος που λειτουργεί η τεχνολογία Blockchain (Πηγή: Nurul, H., Nishchay, J. & Vinay, C. (2018). Blockchain, Cryptocurrency and Bitcoin).

2.3. Εφαρμογές της Τεχνολογίας Blockchain

Όπως γνωρίζουμε, το Bitcoin αποτελεί το πιο δημοφιλές παράδειγμα χρήσης της τεχνολογίας Blockchain. Ωστόσο, η τεχνολογία Blockchain δεν περιορίζεται μόνο στα κρυπτονομίσματα. Σε αυτήν την ενότητα, θα εξετάσουμε μερικές άλλες περιπτώσεις χρήσης της τεχνολογίας αυτής. Αυτές περιλαμβάνουν τα εξής (Subashini, S., & Kavitha, V. (2011)) :

- **Διαχείριση Εφοδιαστικής Αλυσίδας (Supply Chain Management):** Η ροή εργασιών στη SCM περιλαμβάνει μια σειρά υπηρεσιών, όπως η κατασκευή, η αποθήκευση και η παραγωγή, έως και την παράδοση και κατανάλωση των προϊόντων. Δεδομένου ότι εμπλέκονται πολλοί παράγοντες, ο όγκος των δεδομένων που πρέπει να αποθηκευτούν είναι τεράστιος. Κάθε φορά που ένα προϊόν αλλάζει χέρια, οι συναλλαγές καταγράφονται, γεγονός που συμβάλλει στη μείωση των καθυστερήσεων και στην εξάλειψη των ανθρώπινων λαθών. Έτσι, οι παραγγελίες, οι αποδείξεις και οι

ειδοποιήσεις αποστολής μπορούν να παρακολουθούνται με ευκολία. Επιπλέον, τα φυσικά αγαθά μπορούν να συσχετιστούν με σειριακούς αριθμούς, barcodes και ψηφιακές ετικέτες, ενώ οι πληροφορίες μπορούν να κοινοποιούνται αποτελεσματικά μεταξύ προμηθευτών και πωλητών.

- **Διατραπεζικές και Διεθνείς Οικονομικές Συναλλαγές**: Η τεχνολογία Blockchain υιοθετείται από χρηματοπιστωτικά ιδρύματα για πολλούς λόγους. Οι διασυνοριακές συναλλαγές γίνονται σημαντικά πιο γρήγορες και οικονομικά αποδοτικές. Επιπλέον, η αυξημένη ακρίβεια στις συναλλαγές σε συνδυασμό με τη μείωση του χρόνου διακανονισμού, είναι καθοριστικής σημασίας για το εμπόριο μετοχών. Παράλληλα, τα έξυπνα συμβόλαια διασφαλίζουν την ομαλή διεξαγωγή εμπορικών συναλλαγών και συμφωνιών. Ενισχύει επίσης τη διαχείριση ταυτοτήτων, η οποία αποτελεί κρίσιμο παράγοντα για τον τραπεζικό τομέα. Τέλος, η διαφάνεια και η δυνατότητα παρακολούθησης των συναλλαγών συμβάλλουν στη βελτίωση των προγραμμάτων επιβράβευσης και ανταμοιβών, ενισχύοντας τη συνολική αποδοτικότητα.

- **Απόδειξη Ιδιοκτησίας**: Μία από τις πιο κοινές εφαρμογές της τεχνολογίας blockchain είναι η Απόδειξη Ιδιοκτησίας Πνευματικών Δικαιωμάτων. Ένα δημόσιο blockchain μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο ιδιοκτησίας σε μελλοντικό χρόνο, καταγράφοντας το ψηφιακό αντικείμενο και την ταυτότητα του ιδιοκτήτη τη στιγμή της καταχώρισης. Η καταχώριση αυτή γίνεται μέσω ενός hash, ο οποίος προσφέρει επαρκή απόδειξη ιδιοκτησίας.

- **Αποκεντρωμένοι Αυτόνομοι Οργανισμοί**: Βασίζονται σε έξυπνα συμβόλαια για τη λειτουργία τους και δεν διαθέτουν κεντρική διαχείριση. Αντίθετα, οι κανόνες που καθορίζουν τη λειτουργία του οργανισμού ορίζονται μέσα από τα έξυπνα συμβόλαια. Η διαχείριση του οργανισμού πρέπει να γίνεται με αποκεντρωμένο τρόπο, γεγονός που δημιουργεί την ανάγκη για blockchains χωρίς άδειες. Αυτά τα συστήματα συνήθως βασίζονται σε μια ήδη υπάρχουσα τεχνολογία blockchain και συνοδεύονται από το δικό τους ψηφιακό νόμισμα.

- **Καταγραφή Ακινήτων**: Τα δεδομένα που σχετίζονται με την καταγραφή ακινήτων μπορούν να αποθηκευτούν σε μια ασφαλή και διαφανή πλατφόρμα, η οποία

διασφαλίζεται μέσω κρυπτογραφικών πρωτοκόλλων (Petric, G., et al. (2017)). Η εταιρεία ChromaWay έχει ήδη αναπτύξει λύσεις σε αυτόν τον τομέα.

- **Ηλεκτρονική Ψηφοφορία (E-Voting)**: Μία από τις βασικές απαιτήσεις του κοινού για την ηλεκτρονική ψηφοφορία είναι η διασφάλιση της ιδιωτικότητας, καθώς οι ψήφοι πρέπει να παραμένουν ανώνυμες για να αποφευχθεί κάθε είδους εκφοβισμός. Ταυτόχρονα, είναι απαραίτητη η δημόσια επαληθευσιμότητα, ώστε να εξασφαλίζεται η ακεραιότητα της ψηφοφορίας. Δεδομένου ότι στην ψηφοφορία συμμετέχουν πολλά μέρη τα οποία δεν εμπιστεύονται το ένα το άλλο, η τεχνολογία blockchain αποτελεί μια από τις πιο αξιόπιστες λύσεις.

2.4. Προκλήσεις και Περιορισμοί της Τεχνολογίας Blockchain

Η τεχνολογία blockchain αποτελεί μία από τις πιο σημαντικές και καινοτόμες εξελίξεις της σύγχρονης εποχής. Έχει βρει εφαρμογές σε ποικίλους τομείς, όπως τα χρηματοοικονομικά και η υγεία. Ωστόσο, παρά τη διάδοση και την επιρροή της στον τεχνολογικό κόσμο, εξακολουθούν να υπάρχουν αρκετές ανησυχίες και προκλήσεις που τη συνοδεύουν. Ακολουθούν ορισμένες από αυτές τις προκλήσεις που αντιμετωπίζει η τεχνολογία Blockchain (Li, Q., & Clark, G. (2013)).

Επεκτασιμότητα ή Μέγεθος Δικτύου: Καθώς αυξάνεται ο αριθμός των καθημερινών συναλλαγών και κάθε μπλοκ αποθηκεύει δεδομένα ενώ παράγονται συνεχώς νέα μπλοκ, η πρόκληση της επεκτασιμότητας γίνεται πιο έντονη. Εάν ένα blockchain δεν υποστηρίζεται από ένα ιδιαίτερα ισχυρό δίκτυο, είναι πιθανό να παρουσιαστούν αποτυχίες στο σύστημα. Η βελτίωση της αποθήκευσης των blockchains ή ακόμα και ο πλήρης επανασχεδιασμός τους θα μπορούσε να προσφέρει λύσεις στα προβλήματα επεκτασιμότητας.

Ιδιωτικότητα και Ασφάλεια: Στην αρχή, τα blockchains ήταν προσβάσιμα από το κοινό. Όμως στη συνέχεια, για να προστατευτούν τα δεδομένα και να περιοριστεί η πρόσβαση, τα blockchains έγιναν ελεγχόμενα, το οποίο προϋποθέτει σημαντική προετοιμασία και σχεδιασμό.

Διαρροή Ιδιωτικότητας: Δεν προσφέρεται πλήρη εγγύηση για την ιδιωτικότητα των συναλλαγών, καθώς οι συναλλαγές με Bitcoin ενδέχεται να εκθέσουν προσωπικά δεδομένα των χρηστών (Miller, K. W., Voas, J., & Hurlburt, G. F. (2012)). Παρά τη χρήση firewall (τοίχος προστασίας) και Network Address Translators (Μεταφραστές Διευθύνσεων Δικτύου), οι διευθύνσεις IP μπορούν να εντοπιστούν και να συσχετιστούν με τα ψευδώνυμα των χρηστών. Ωστόσο, ένας πιθανός τρόπος να αντιμετωπιστεί αυτό το πρόβλημα είναι η ανωνυμία.

Ανθρώπινο Σφάλμα: Τα δεδομένα που αποθηκεύονται στο blockchain ενδέχεται να μην είναι απολύτως αξιόπιστα, γι' αυτό είναι σημαντικό τα γεγονότα να καταγράφονται με ακρίβεια.

Αρχικό Κόστος: Η αρχική υλοποίηση της τεχνολογίας blockchain είναι δαπανηρή, καθώς απαιτεί κόστος για το λογισμικό και την εξειδίκευση του προσωπικού. Επιπλέον, η υψηλή ζήτηση σε συνδυασμό με την περιορισμένη προσφορά αυξάνουν περαιτέρω το κόστος.

Κατανάλωση Ενέργειας: Η διαδικασία επικύρωσης των συναλλαγών στο blockchain απαιτεί την εκτέλεση πολύπλοκων μαθηματικών αλγορίθμων για την επαλήθευση των συναλλαγών και τη διασφάλιση του δικτύου, καταναλώνοντας με αυτόν τον τρόπο σημαντική ποσότητα ισχύος και ενέργειας.

Πολυπλοκότητα: Το λεξιλόγιο που εισάγει η τεχνολογία Blockchain περιλαμβάνει πολλούς τεχνικούς όρους. Γι’ αυτό το λόγο οι άνθρωποι που ασχολούνται με δραστηριότητες σχετικές με αυτή την τεχνολογία χρειάζεται να εξοικειωθούν με αυτές τις εκφράσεις.

Εγωιστική Εξόρυξη (Selfish Mining): Η εγωιστική εξόρυξη προκαλεί ανασφάλεια στα blockchains, καθώς εκμεταλλεύεται μια μικρή ποσότητα υπολογιστικής ισχύος για να καταστήσει το δίκτυο ευάλωτο. Οι εξορύκτες που ακολουθούν αυτή την πρακτική κρατούν τα εξορυγμένα μπλοκ χωρίς να τα μεταδίδουν άμεσα, και το κοινό μπορεί να έχει πρόσβαση στον ιδιωτικό κλάδο μόνο υπό συγκεκριμένες συνθήκες. Έτσι, οι "εγωιστές" εξορύκτες έχουν τη δυνατότητα να δημιουργούν ιδιωτικές αλυσίδες χωρίς να ανησυχούν για τον ανταγωνισμό, διασφαλίζοντας έτσι μεγαλύτερα κέρδη.

Ενσωμάτωση με Παλιότερα Συστήματα: Η μετάβαση σε ένα σύστημα βασισμένο σε blockchain μπορεί να πραγματοποιηθεί είτε με την πλήρη ανακατασκευή του συστήματος (δημιουργία ενός νέου συστήματος με βάση το blockchain) είτε με την ενσωμάτωση της τεχνολογίας Blockchain στο υπάρχον σύστημα. Επειδή η κατάργηση των παλαιότερων συστημάτων μπορεί να είναι δύσκολη, μια πιο πρακτική προσέγγιση είναι η τροποποίηση του υπάρχοντος συστήματος ώστε να υποστηρίζει την τεχνολογία Blockchain. Αυτή η διαδικασία μπορεί να απαιτήσει χρόνο, χρήματα και εξειδικευμένες δεξιότητες.

Δημόσια Αντίληψη: Δεδομένου ότι η τεχνολογία Blockchain είναι σχετικά καινούργια, πολλοί άνθρωποι δεν την γνωρίζουν καλά και την ταυτίζουν με τα bitcoins. Επομένως, είναι σημαντικό να ενημερωθεί το κοινό σχετικά με αυτήν.

2.5. Το Μέλλον της Τεχνολογίας Blockchain

Είναι γνωστό ότι τεχνολογίες όπως το blockchain μπορούν να μειώσουν τους κινδύνους στον κυβερνοχώρο, κάτι που αποτελεί παγκόσμιο ζήτημα. Επιπλέον, το blockchain έχει ήδη εφαρμοστεί σε διάφορες βιομηχανίες, προσφέροντας σημαντικά πλεονεκτήματα. Έτσι, καθώς όλο και περισσότερες οργανώσεις υιοθετούν αυτήν την τεχνολογία, είναι πιθανό ότι θα διαμορφώσει το μέλλον του διαδικτύου. Παράλληλα, με την αύξηση της δημοτικότητας των κρυπτονομισμάτων και την ενσωμάτωση μεθόδων blockchain από χρηματοπιστωτικά ιδρύματα, το παγκόσμιο τραπεζικό σύστημα θα μπορούσε να υποστεί σημαντικές αλλαγές. Συνεπώς, αξίζει να εξετάσουμε πώς αυτή η τεχνολογία θα επηρεάσει το μέλλον (Li, Q. & Clark, G. (2013)).

- Δοκιμή Blockchain: Για να αποτραπεί η παραπλάνηση των χρηστών μέσω παραποιημένων αποδόσεων των blockchains, είναι απαραίτητο να επιλέγεται το κατάλληλο blockchain που ανταποκρίνεται στις επιχειρηματικές ανάγκες. Αυτό καθιστά τη δοκιμή του blockchain ζωτικής σημασίας. Η διαδικασία αυτή περιλαμβάνει δύο κύριες φάσεις. Αρχικά, στη φάση τυποποίησης (standardization phase), τα blockchains αξιολογούνται με βάση συγκεκριμένα κριτήρια για να επιβεβαιωθεί η εγκυρότητά τους. Στη συνέχεια, στη φάση δοκιμής (testing phase), τα blockchains υποβάλλονται σε ελέγχους βάσει διαφόρων κριτηρίων, προκειμένου να εξασφαλιστεί η αξιοπιστία τους.

- Εξάλειψη της διαδικασίας κεντρικοποίησης: Παρόλο που η τεχνολογία blockchain στηρίζεται στην αρχή της αποκέντρωσης, η εγωιστική εξόρυξη θα μπορούσε να διευκολύνει την εκμετάλλευση της επίθεσης του 51%. Αυτό θα αναιρούσε τον στόχο της αποκέντρωσης, γι' αυτό είναι απαραίτητο να προταθούν κάποιες λύσεις για την αντιμετώπιση αυτού του προβλήματος.

- Ανάλυση Μεγάλων Δεδομένων (Big Data): Όταν τα Big Data συνδυάζονται με blockchains, μπορούν να ενισχύσουν τη διαχείριση και την ανάλυση δεδομένων. Η διαχείριση δεδομένων διασφαλίζει την αποθήκευση και την προστασία των δεδομένων, ενώ η ανάλυση δεδομένων επιτρέπει την αποτελεσματική διαχείριση των συναλλαγών.

- Διάφορες εφαρμογές του Blockchain: Παραδοσιακοί οργανισμοί θα μπορούσαν να υιοθετήσουν τα blockchains για να βελτιώσουν τη λειτουργία των συστημάτων τους. Η εφαρμογή των έξυπνων συμβολαίων σε συνδυασμό με τα blockchains θα μπορούσε επίσης να ενισχύσει αυτήν τη διαδικασία.

- Τραπεζικός τομέας: Τα blockchains θα μπορούσαν να αντικαταστήσουν τις κεντρικές τράπεζες στο προσεχές μέλλον. Η τεχνολογία Blockchain έχει τη δυνατότητα να μειώσει το κόστος υποδομής, να βελτιώσει τις διασυνοριακές πληρωμές και να διευκολύνει τις συναλλαγές τίτλων με μεγαλύτερη ασφάλεια.

- Βιομηχανίες: Έχουν τη δυνατότητα να ανοίξουν νέες προοπτικές για τη βιομηχανία και να μετασχηματίσουν τις υπάρχουσες δομές. Οι συναλλαγές θα γίνονται γρήγορα και αποτελεσματικά, εξαλείφοντας την ανάγκη για μεσάζοντες μεταξύ των δύο εμπλεκόμενων μερών.

- Κυβερνήσεις: Τα κρυπτονομίσματα ενδέχεται να επηρεάσουν τα χρηματοοικονομικά συστήματα σε πολλές χώρες. Επιπλέον, η ανθρώπινη συμμετοχή στη διαδικασία αυθεντικοποίησης θα μπορούσε να καταργηθεί πλήρως.

- Καταπολέμηση του εγκλήματος: Η τεχνολογία Blockchain, ως λογισμικό, διαθέτει τη δυνατότητα να εντοπίζει εγκληματίες και φαίνεται πως θα είναι πολύ πιο οικονομική σε σύγκριση με τις τρέχουσες μεθόδους.

ΚΕΦΑΛΑΙΟ 3. ΟΙΚΟΝΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΤΩΝ ΨΗΦΙΑΚΩΝ ΝΟΜΙΣΜΑΤΩΝ

3.1. Τρέχον Μερίδιο Αγοράς

Η ραγδαία άνοδος των ψηφιακών νομισμάτων τα τελευταία χρόνια έχει φέρει σημαντικές αλλαγές στις παγκόσμιες αγορές, προκαλώντας το έντονο ενδιαφέρον επενδυτών, κυβερνήσεων και χρηματοπιστωτικών ιδρυμάτων. Ειδικότερα, τα ψηφιακά νομίσματα, με το Bitcoin να ηγείται της κίνησης, έχουν μεταβάλει το παραδοσιακό χρηματοπιστωτικό σύστημα, δημιουργώντας νέες ευκαιρίες αλλά και προκλήσεις. Παράλληλα, το μερίδιο αγοράς των ψηφιακών νομισμάτων, όπως το Bitcoin, το Ethereum και άλλων, αυξάνεται συνεχώς, αναδεικνύοντας την ισχυρή ζήτηση και την εμπιστοσύνη των επενδυτών σε αυτά τα νέα χρηματοοικονομικά μέσα. Αυτή η εξέλιξη έχει ενισχύσει τη σημασία τους στην παγκόσμια οικονομία, καθώς και το ενδιαφέρον των εμπλεκόμενων φορέων που αναγνωρίζουν τη δυνατότητα των ψηφιακών νομισμάτων να επηρεάσουν βαθιά τον τρόπο λειτουργίας των παραδοσιακών αγορών.

3.1.1. Κεφαλαιοποίηση της Αγοράς των Ψηφιακών Νομισμάτων

Σε αυτό το πλαίσιο, η κεφαλαιοποίηση της αγοράς, γνωστή και ως market cap, είναι ένα εξαιρετικά σημαντικό εργαλείο στον κόσμο των ψηφιακών νομισμάτων, καθώς βοηθάει τους επενδυτές να κατανοήσουν τη συνολική αξία ενός κρυπτονομίσματος στην αγορά. Ο δείκτης αυτός υπολογίζεται πολλαπλασιάζοντας την τρέχουσα τιμή ενός κρυπτονομίσματος με τον συνολικό αριθμό των νομισμάτων του που έχουν εξορυχθεί (mined).
Αποτελεί έναν κρίσιμο δείκτη στον κόσμο των κρυπτονομισμάτων, καθώς επιτρέπει στους χρήστες να αξιολογήσουν το μέγεθος και τις προοπτικές ανάπτυξης ψηφιακών νομισμάτων, όπως το Bitcoin. Μέσω της κατηγοριοποίησής τους, όπου τα ψηφιακά νομίσματα ταξινομούνται βάσει του μεγέθους τους, διευκολύνεται η διαφοροποίηση των κρυπτονομισμάτων. Αυτή η κατηγοριοποίηση λαμβάνει υπόψη τα διαφορετικά επίπεδα κινδύνου, τις δυνατότητες εξέλιξής τους και τα αντίστοιχα εύρη αξίας τους.

Γενικά, όταν ένα κρυπτονόμισμα έχει μεγαλύτερη κεφαλαιοποίηση, είναι συνήθως πιο εύκολο να αγοραστεί ή να πωληθεί, δηλαδή παρουσιάζει μεγαλύτερη ρευστότητα, ενώ η τιμή του δεν παρουσιάζει γρήγορες διακυμάνσεις, κάτι που συνεπάγεται χαμηλότερο ρίσκο. Η κατανόηση αυτού του βασικού όρου είναι εξαιρετικά σημαντική για όσους επιδιώκουν να επενδύσουν σε κρυπτονομίσματα. Συγκεκριμένα, το market cap λειτουργεί ως δείκτης που αντανακλά τη δημοφιλία και τη σημασία ενός ψηφιακού νομίσματος μέσα στο ευρύτερο ψηφιακό οικοσύστημα σε οποιαδήποτε στιγμή. Γι' αυτόν τον λόγο, ακολουθούν μερικοί λόγοι για τους οποίους το market cap έχει τόσο μεγάλη σημασία στον κόσμο των κρυπτονομισμάτων:

Σχετικό Μέγεθος: Η κεφαλαιοποίηση της αγοράς όχι μόνο δίνει τη δυνατότητα να εκτιμηθεί το σχετικό μέγεθος ενός κρυπτονομίσματος σε σχέση με την ευρύτερη αγορά, αλλά επίσης προσφέρει στους επενδυτές μια τυποποιημένη μέθοδο για να αξιολογήσουν πόσο μεγάλο ή μικρό είναι ένα κρυπτονόμισμα σε σύγκριση με άλλα.

Αξιολόγηση Κινδύνου: Η γνώση της κεφαλαιοποίησης της αγοράς ενός κρυπτονομίσματος συμβάλλει στην αξιολόγηση του κινδύνου του. Οι μεγαλύτερες κεφαλαιοποιήσεις συχνά υποδηλώνουν λιγότερο ασταθή περιουσιακά στοιχεία, ενώ οι μικρότερες κεφαλαιοποιήσεις μπορεί να υποδεικνύουν υψηλότερο κίνδυνο και μεγαλύτερη μεταβλητότητα.

Δείκτης Ρευστότητας: Η κεφαλαιοποίηση της αγοράς μπορεί να λειτουργεί ως ένδειξη της ρευστότητας ενός κρυπτονομίσματος, καθώς δείχνει πόσο εύκολα μπορεί ένα token να ανταλλαχθεί με άλλα κρυπτονομίσματα. Επιπλέον, τα κρυπτονομίσματα με υψηλότερη κεφαλαιοποίηση και μεγαλύτερη ρευστότητα συνήθως έχουν αυξημένους όγκους συναλλαγών, γεγονός που τα καθιστά πιο εύκολα στην αγορά και πώληση όχι μόνο σε ανταλλακτήρια, αλλά και σε πορτοφόλια και διάφορες πλατφόρμες συναλλαγών.

Εμπιστοσύνη των Επενδυτών: Η κεφαλαιοποίηση της αγοράς παίζει καθοριστικό ρόλο για πολλούς επενδυτές όταν εξετάζουν τη βιωσιμότητα ενός κρυπτονομίσματος ως επιλογή για επένδυση. Παράλληλα, παράγοντες όπως η κεφαλαιοποίηση και η θέση ενός κρυπτονομίσματος στην αγορά διευκολύνουν τον εντοπισμό επενδυτικών ευκαιριών, την εκτίμηση του κινδύνου, καθώς και την αποδοχή ενός token από την κοινότητα των κρυπτονομισμάτων.

Συνεπώς, η κεφαλαιοποίηση της αγοράς αποτελεί έναν κρίσιμο δείκτη που επηρεάζει τις επενδυτικές στρατηγικές στον χώρο των ψηφιακών νομισμάτων. Συγκεκριμένα, βοηθά τους επενδυτές να λαμβάνουν ενημερωμένες αποφάσεις, να αναπτύσσουν ολοκληρωμένες στρατηγικές και να αξιολογούν τόσο το αναπτυξιακό δυναμικό όσο και τους κινδύνους που συνδέονται με συγκεκριμένα ψηφιακά περιουσιακά στοιχεία.
Για τον λόγο αυτό, όταν οι επενδυτές αξιολογούν ένα ψηφιακό νόμισμα, ξεκινούν από αυτόν τον δείκτη. Παρόλα αυτά, η προσέγγισή τους ποικίλλει ανάλογα με τους επενδυτικούς στόχους και την ανοχή τους στον κίνδυνο. Ας εξετάσουμε όμως, πώς η κεφαλαιοποίηση της αγοράς επηρεάζει τη λήψη αποφάσεων μέσω τριών βασικών παραμέτρων:

Δυνατότητα ανάπτυξης: Τα ψηφιακά νομίσματα με μικρότερη κεφαλαιοποίηση συχνά προσφέρουν μεγαλύτερες προοπτικές ανάπτυξης σε σύγκριση με εκείνα που έχουν μεγαλύτερη κεφαλαιοποίηση. Οι επενδυτές που επιδιώκουν υψηλό ρίσκο με την προσδοκία υψηλών αποδόσεων μπορεί να εστιάσουν σε αυτά, επιδιώκοντας σημαντικά κέρδη.

Αξιολόγηση Κινδύνου: Η κεφαλαιοποίηση της αγοράς επιτρέπει στους επενδυτές να εκτιμήσουν το επίπεδο κινδύνου που συνδέεται με μια επένδυση σε ψηφιακά νομίσματα. Γενικά, τα ψηφιακά νομίσματα με μεγαλύτερη κεφαλαιοποίηση θεωρούνται πιο σταθερά, χάρη στις καθιερωμένες επιδόσεις τους και την ευρύτερη αποδοχή τους.

Διαφοροποίηση: Για τη διαχείριση του κινδύνου, οι επενδυτές μπορεί να επιλέξουν να κατανείμουν τα κεφάλαιά τους σε διάφορες κατηγορίες κεφαλαιοποίησης, συμπεριλαμβανομένων των ψηφιακών νομισμάτων με μεγάλη, μεσαία και μικρή κεφαλαιοποίηση.

Συνοψίζοντας, παρόλο που το market cap αποτελεί έναν σημαντικό δείκτη, δεν πρέπει να είναι ο μοναδικός παράγοντας στις επενδυτικές αποφάσεις, καθώς παραβλέπει κρίσιμα στοιχεία όπως την ιστορική απόδοση του νομίσματος και τον ανταγωνισμό στην αγορά.

3.1.2. Τρέχον Μερίδιο Αγοράς των Ψηφιακών Νομισμάτων

Στον χώρο των ψηφιακών νομισμάτων, οι στρατηγικές επένδυσης μπορεί να διαφέρουν σημαντικά με βάση την κατηγορία κεφαλαιοποίησης. Οι βασικές κατηγορίες κεφαλαιοποίησης περιλαμβάνουν: μεγάλη, μεσαία και μικρή κεφαλαιοποίηση, καθεμία από τις οποίες διαθέτει μοναδικά χαρακτηριστικά και διαφορετικές προσεγγίσεις για επενδύσεις.

Ψηφιακά νομίσματα μεγάλης κεφαλαιοποίησης (Large-Cap)

Τα ψηφιακά νομίσματα μεγάλης κεφαλαιοποίησης έχουν αξία που ξεπερνά τα 10 δισεκατομμύρια δολάρια και περιλαμβάνουν δημοφιλή ονόματα όπως το Bitcoin (BTC), το Ethereum (ETH), το Tether (USDT), το Binance Coin (BNB), το Solana (SOL), το USD Coin (USDC) και το XRP (Εικόνα 4). Λόγω της σταθερής τους απόδοσης και της εκτεταμένης αποδοχής που έχουν κερδίσει, πολλοί επενδυτές επιλέγουν να τα διατηρούν στο χαρτοφυλάκιό τους για μακροπρόθεσμες επενδύσεις. Εστιάζοντας ένα σημαντικό μέρος των επενδύσεών τους σε νομίσματα μεγάλης κεφαλαιοποίησης, οι επενδυτές μπορούν να μειώσουν τον κίνδυνο και να αξιοποιήσουν τις δυναμικές αποδόσεις που αυτά τα νομίσματα προσφέρουν.

Τέλος, τα ψηφιακά νομίσματα μεγάλης κεφαλαιοποίησης είναι λιγότερο πιθανό να παρουσιάσουν ακραίες διακυμάνσεις τιμών, αλλά ενδέχεται να προσφέρουν πιο μέτριες αποδόσεις σε σύγκριση με εκείνα μικρότερης κεφαλαιοποίησης.

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$63,273.72	0.60%	1.37%	7.32%	$1,249,367,015,503	$26,445,380,101 416,123 BTC	19,745,434 BTC	
2	Ethereum ETH	$2,692.98	1.24%	2.84%	3.30%	$323,963,008,860	$11,642,745,586 4,298,520 ETH	120,299,121 ETH	
3	Tether USDT	$1.00	0.01%	0.01%	0.00%	$117,900,178,096	$48,770,529,734 48,752,738,552 USDT	117,862,094,160 USDT	
4	BNB BNB	$555.82	0.95%	3.67%	0.55%	$81,113,745,451	$1,749,697,365 3,136,349 BNB	145,935,303 BNB	
5	Solana SOL	$156.42	0.98%	1.89%	8.81%	$72,915,503,894	$2,486,456,846 15,879,088 SOL	466,162,150 SOL	
6	USDC USDC	$0.9999	0.01%	0.01%	0.01%	$34,631,961,281	$5,194,149,643 5,194,079,590 USDC	34,632,515,167 USDC	
7	XRP XRP	$0.5809	1.88%	3.42%	3.19%	$32,635,282,545	$1,029,708,952 1,761,783,136 XRP	56,180,094,752 XRP	
8	Dogecoin DOGE	$0.1054	1.84%	4.11%	4.54%	$15,363,286,724	$525,699,349 4,952,622,331 DOGE	145,696,356,384 DOGE	
9	TRON TRX	$0.1649	0.37%	0.11%	17.01%	$14,320,294,076	$805,612,826 4,879,357,237 TRX	86,834,005,878 TRX	
10	Toncoin TON	$5.44	2.64%	6.30%	20.09%	$13,786,166,360	$904,236,802 165,077,466 TON	2,534,753,941 TON	

Εικόνα 4. Τα κρυπτονομίσματα με τη μεγαλύτερη κεφαλαιοποίηση (Πηγή: CoinMarketCap.com, Αύγουστος 2024).

Ψηφιακά νομίσματα μεσαίας κεφαλαιοποίησης (Mid-Cap)

Τα ψηφιακά νομίσματα μεσαίας κεφαλαιοποίησης έχουν αξία που κυμαίνεται από 1 έως 10 δισεκατομμύρια δολάρια και περιλαμβάνουν κρυπτονομίσματα όπως το Shiba Inu (SHIB), το Chainlink (LINK), το Bitcoin Cash (BCH) και το Polkadot (DOT) (Εικόνα 5). Αυτά τα νομίσματα συχνά επιλέγονται από τους επενδυτές λόγω των αναπτυξιακών τους δυνατοτήτων και τους προσφέρουν κατάλληλες ευκαιρίες για επενδύσεις. Επιπλέον, ενώ αυτά τα νομίσματα προσφέρουν σημαντική ανατίμηση της τιμή, συνοδεύονται από υψηλότερο κίνδυνο, σε σύγκριση με τα νομίσματα μεγάλης κεφαλαιοποίησης.

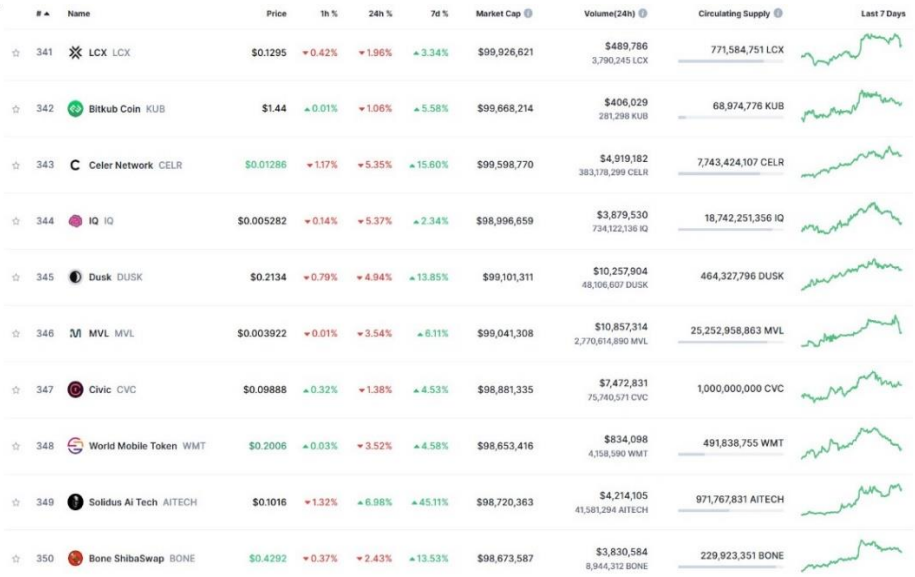
#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
13	Shiba Inu SHIB	$0.00001441	1.81%	4.57%	9.87%	$8,488,789,684	$228,739,290 15,746,037,634,962 SHIB	589,270,237,439,662 SHIB	
14	Chainlink LINK	$12.00	1.74%	1.03%	19.71%	$7,294,752,082	$273,466,820 22,532,366 LINK	608,099,970 LINK	
15	Bitcoin Cash BCH	$341.81	2.23%	4.95%	1.86%	$6,751,419,592	$207,598,947 594,889 BCH	19,752,175 BCH	
16	Polkadot DOT	$4.56	1.84%	5.89%	2.89%	$6,774,925,024	$116,205,304 25,189,221 DOT	1,485,888,535 DOT	
17	UNUS SED LEO LEO	$5.79	0.10%	3.45%	1.49%	$5,359,646,983	$1,871,827 320,962 LEO	925,640,368 LEO	
18	NEAR Protocol NEAR	$4.73	2.17%	3.82%	21.23%	$5,293,235,805	$221,326,603 46,127,110 NEAR	1,119,326,611 NEAR	
19	Dai DAI	$0.9997	0.02%	0.03%	0.02%	$5,363,927,271	$84,650,505 84,659,064 DAI	5,365,382,703 DAI	
20	Polygon MATIC	$0.5033	2.00%	4.91%	18.25%	$5,016,228,451	$278,707,891 548,159,513 MATIC	9,966,217,903 MATIC	
21	Litecoin LTC	$63.19	1.69%	2.87%	4.78%	$4,732,960,469	$230,543,951 3,608,542 LTC	74,905,612 LTC	
22	Kaspa KAS	$0.168	0.96%	1.04%	6.20%	$4,122,312,733	$56,004,318 331,296,384 KAS	24,541,700,380 KAS	

Εικόνα 5. Τα κρυπτονομίσματα μεσαίας κεφαλαιοποίησης (Πηγή: CoinMarketCap.com, Αύγουστος 2024).

Ψηφιακά νομίσματα μικρής κεφαλαιοποίησης (Small-Cap)

Τα ψηφιακά νομίσματα μικρής κεφαλαιοποίησης έχουν αξία που κυμαίνεται κάτω από 100 εκατομμύρια δολάρια και περιλαμβάνουν κρυπτονομίσματα όπως το LCX, το Bitkub Coin (KUB) και το Dusk (Εικόνα 6). Οι επενδυτές μπορεί να επιλέξουν νομίσματα μικρής κεφαλαιοποίησης, με την ελπίδα να αποκομίσουν σημαντικά κέρδη αν αυτά επιτύχουν. Ωστόσο, επειδή τα ψηφιακά νομίσματα μικρής κεφαλαιοποίησης χαρακτηρίζονται συχνά από υψηλή

μεταβλητότητα, θεωρούνται κερδοσκοπικές επενδύσεις. Γι' αυτόν τον λόγο, οι επενδυτές πρέπει να είναι προετοιμασμένοι για σημαντικές διακυμάνσεις στις τιμές.



#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
341	LCX LCX	$0.1295	0.42%	1.96%	3.34%	$99,926,621	$489,786 3,790,245 LCX	771,584,751 LCX	
342	Bitkub Coin KUB	$1.44	0.01%	1.06%	5.58%	$99,668,214	$406,029 281,298 KUB	68,974,776 KUB	
343	Celer Network CELR	$0.01286	1.17%	5.35%	15.60%	$99,598,770	$4,919,182 383,178,299 CELR	7,743,424,107 CELR	
344	IQ IQ	$0.005282	0.14%	5.37%	2.34%	$98,996,659	$3,879,530 734,122,136 IQ	18,742,251,356 IQ	
345	Dusk DUSK	$0.2134	0.79%	4.94%	13.85%	$99,101,311	$10,257,904 48,106,607 DUSK	464,327,796 DUSK	
346	MVL MVL	$0.003922	0.01%	3.54%	8.11%	$99,041,308	$10,857,314 2,770,614,890 MVL	25,252,958,863 MVL	
347	Civic CVC	$0.09888	0.32%	1.38%	4.53%	$98,881,335	$7,472,831 75,740,571 CVC	1,000,000,000 CVC	
348	World Mobile Token WMT	$0.2006	0.03%	3.52%	4.58%	$98,653,416	$834,098 4,158,590 WMT	491,838,755 WMT	
349	Solidus Ai Tech AITECH	$0.1016	1.32%	6.98%	45.11%	$98,720,363	$4,214,105 41,581,294 AITECH	971,767,831 AITECH	
350	Bone ShibaSwap BONE	$0.4292	0.37%	2.43%	13.53%	$98,673,587	$3,830,584 8,944,312 BONE	229,923,351 BONE	

Εικόνα 6. Τα κρυπτονομίσματα μικρής κεφαλαιοποίησης (Πηγή: CoinMarketCap.com, Αύγουστος 2024).

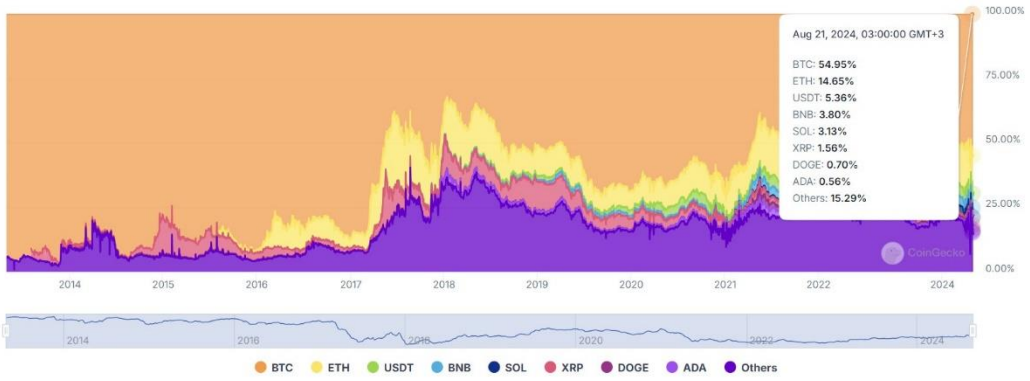
Στο πλαίσιο αυτό, η κυριαρχία του Bitcoin αποτυπώνεται ξεκάθαρα στο παρακάτω γράφημα (Εικόνα 7), το οποίο παρουσιάζει τη σχέση του με τα άλλα κρυπτονομίσματα που ανήκουν στα 10 κορυφαία της αγοράς. Το γράφημα καταγράφει το ποσοστό συμμετοχής του Bitcoin και των άλλων κρυπτονομισμάτων στη συνολική κεφαλαιοποίηση της αγοράς από το 2014 έως το 2024.

Αναλυτικότερα, παρατηρούμε ότι από τον Ιανουάριο του 2014, το Bitcoin κατείχε σχεδόν το 90% της συνολικής κεφαλαιοποίησης της αγοράς κρυπτονομισμάτων. Ωστόσο, με την εισαγωγή και την άνοδο άλλων κρυπτονομισμάτων, η κυριαρχία του μειώθηκε σημαντικά με την πάροδο των ετών. Παρά τη μείωση αυτή, το Bitcoin διατηρεί μέχρι σήμερα τον κυρίαρχο ρόλο του στην αγορά, κατέχοντας το 54.95% της συνολικής κεφαλαιοποίησης, τον Αύγουστο του 2024. Αυτό το γεγονός υπογραμμίζει την ανθεκτικότητα και τη σημασία του Bitcoin ως το πρωτοπόρο κρυπτονόμισμα, παρά τις προκλήσεις και τις ανταγωνιστικές πιέσεις από άλλα ψηφιακά περιουσιακά στοιχεία.

Όσον αφορά τα άλλα κρυπτονομίσματα, ιδιαίτερα του Ethereum, συνέβαλε στη μείωση της κυριαρχίας του Bitcoin. Απ’ ότι βλέπουμε, το Ethereum κατέχει περίπου το 15% της αγοράς,

καθιστώντας το το δεύτερο μεγαλύτερο κρυπτονόμισμα μετά το Bitcoin. Η παρουσία του Tether (USDT) με μερίδιο κοντά στο 5%, υποδεικνύει τη σημαντική θέση των stablecoins στην αγορά, τα οποία προσφέρουν σταθερότητα σε μια αγορά γνωστή για την υψηλή μεταβλητότητά της. Επίσης, το Binance Coin (BNB) κατέχει περίπου το 4%, το Solana (SOL) το 3%, και το XRP κατέχει περίπου το 2%, αναδεικνύοντας τη διαφοροποίηση των κορυφαίων κρυπτονομισμάτων.

Σχετικά με τα υπόλοιπα κρυπτονομίσματα, αντιπροσωπεύουν το 15% της αγοράς για το έτος 2024, το οποίο δείχνει τη σημαντική συμμετοχή των μικρότερων ή αναδυόμενων κρυπτονομισμάτων στην αγορά.



Εικόνα 7. Μερίδιο Αγοράς του Bitcoin και των Κορυφαίων Κρυπτονομισμάτων (2014-2024) (Πηγή: CoinGecko.com).

Παρά τον έντονο ανταγωνισμό, το Bitcoin διατηρεί την κυριαρχία του, κυρίως λόγω της ευρείας αναγνωρισιμότητάς του και της θέσης του ως "ψηφιακού χρυσού" (Taskinsoy, J. (2021)). Ωστόσο, και το Ethereum έχει καταφέρει να αυξήσει το μερίδιο αγοράς του, κυρίως λόγω της πλατφόρμας του που υποστηρίζει την ανάπτυξη αποκεντρωμένων εφαρμογών και πρωτοκόλλων DeFi (Αποκεντρωμένης Χρηματοδότησης).

Παράλληλα, τα Altcoins όπως το BNB και το SOL έχουν επίσης σημειώσει σημαντική άνοδο, προσελκύοντας το ενδιαφέρον των επενδυτών χάρη στις καινοτόμες λύσεις που προτείνουν για προβλήματα όπως η ταχύτητα των συναλλαγών και η ενεργειακή κατανάλωση, τα οποία ταλαιπωρούν τα παραδοσιακά κρυπτονομίσματα.

3.2. Παράγοντες που επηρεάζουν το Μερίδιο Αγοράς

Το μερίδιο αγοράς των ψηφιακών νομισμάτων υπόκειται σε σημαντικές διακυμάνσεις, επηρεαζόμενο από παράγοντες όπως οι τεχνολογικές εξελίξεις, οι ρυθμιστικές αλλαγές, οι γενικότερες συνθήκες της αγοράς, αλλά και κοινωνικοί παράγοντες (Aggarwal, G. et al. (2019)). Επιπλέον, ορισμένοι παράγοντες που μπορεί να επηρεάζουν την τιμή των κρυπτονομισμάτων περιλαμβάνουν την κυρίαρχη εξάρτησή τους από το συναίσθημα της αγοράς και την απουσία ρυθμιστικής εποπτείας. Επειδή η αγορά των κρυπτονομισμάτων είναι εξαιρετικά ελεύθερη και μη ρυθμιζόμενη, αυτό επιτρέπει τη χειραγώγηση της αγοράς από ορισμένους βασικούς παίκτες που κατέχουν μεγάλο ποσοστό των συνολικών κρυπτονομισμάτων. Επιπρόσθετα, η νοοτροπία του κοπαδιού, όπου χιλιάδες επενδυτές επενδύουν και αποσύρουν τα κεφάλαιά τους από φόβο για απώλειες, παίζει επίσης σημαντικό ρόλο στις διακυμάνσεις των τιμών (Linuma, A. (2018)). Ας εξετάσουμε πιο αναλυτικά μερικούς από αυτούς τους παράγοντες:

Αποκέντρωση

Η αποκέντρωση αποτελεί θεμελιώδη πτυχή στο οικοσύστημα των ψηφιακών νομισμάτων και επηρεάζει καθοριστικά το μερίδιο αγοράς τους. Δίκτυα όπως το Bitcoin και το Ethereum, που λειτουργούν με αποκεντρωμένη δομή, προσφέρουν μεγαλύτερη ασφάλεια και ανθεκτικότητα απέναντι σε επιθέσεις και χειραγώγηση. Αυτή η αποκεντρωμένη προσέγγιση έχει ενισχύσει την εμπιστοσύνη των επενδυτών και των χρηστών, συμβάλλοντας σημαντικά στην αύξηση του μεριδίου αγοράς αυτών των νομισμάτων.

Από την άλλη, υπάρχουν και δίκτυα με πιο συγκεντρωτικό χαρακτήρα, όπως το Binance, τα οποία προσφέρουν γρηγορότερες συναλλαγές και χαμηλότερα τέλη. Αν και αυτά τα δίκτυα δέχονται κριτική για την έλλειψη πλήρους αποκέντρωσης, έχουν καταφέρει να αποσπάσουν σημαντικό μερίδιο αγοράς λόγω των πρακτικών τους πλεονεκτημάτων.

Circulating Supply vs Total Supply

Το Circulating Supply αναφέρεται στον αριθμό των νομισμάτων που είναι άμεσα διαθέσιμα για διαπραγμάτευση, εξαιρώντας τα tokens που βρίσκονται στα χέρια των ιδρυτών του έργου, είναι κλειδωμένα σε έξυπνα συμβόλαια ή δεν είναι προσβάσιμα με άλλον τρόπο. Από την άλλη

πλευρά, το Total Supply αναφέρεται στον μέγιστο αριθμό tokens που θα δημιουργηθούν ποτέ στο blockchain, συμπεριλαμβανομένων αυτών που δεν έχουν ακόμη κυκλοφορήσει στο κοινό. Ορισμένα κρυπτονομίσματα, όπως το Bitcoin, έχουν σταθερή συνολική προσφορά, ενώ άλλα μπορεί να περιλαμβάνουν μηχανισμούς για την αύξηση της προσφοράς τους με την πάροδο του χρόνου.

Τιμή ανά Token Κρυπτονομίσματος

Η αξία ενός token καθορίζεται από την τρέχουσα εμπορεύσιμη τιμή του σε ένα συγκεκριμένο νόμισμα, όπως το δολάριο ή το ευρώ. Ακόμη και μικρές διακυμάνσεις στην τιμή του token μπορούν να έχουν σημαντική επίδραση στην κεφαλαιοποίηση της αγοράς, με αποτέλεσμα να προκαλούν αξιόλογες μεταβολές στη συνολική της αξία. Γενικά, όταν η τιμή του token αυξάνεται, η κεφαλαιοποίηση της αγοράς ενισχύεται, ενώ αντίθετα, η μείωση της τιμής οδηγεί σε μείωση της κεφαλαιοποίησης.

Όγκος Συναλλαγών

Ο όγκος συναλλαγών καταγράφει το συνολικό ποσό ενός κρυπτονομίσματος που διακινείται μέσα σε ένα συγκεκριμένο χρονικό διάστημα, συνήθως εντός 24 ωρών. Ένας υψηλός όγκος συναλλαγών συσχετίζεται συχνά με κρυπτονομίσματα μεγάλης κεφαλαιοποίησης και υποδηλώνει μια ρευστή και δραστήρια αγορά. Αντίθετα, ένας χαμηλός όγκος συναλλαγών μπορεί να καταστήσει δύσκολη τη διατήρηση μιας σταθερής κεφαλαιοποίησης στην αγορά. Επίσης, είναι σημαντικό να εξετάζεται η ποιότητα του όγκου συναλλαγών, καθώς ορισμένα ανταλλακτήρια ενδέχεται να συμμετέχουν σε πρακτικές όπως εικονικές συναλλαγές ή άλλες παραπλανητικές μεθόδους. Ωστόσο, οι Balcilar, Bouri, Gupta και Roubaud (2017) διαπίστωσαν ότι ο όγκος συναλλαγών μπορεί να προβλέψει τις αποδόσεις, αλλά δεν επηρεάζει την τιμή.

Οικονομικοί Παράγοντες

Το γενικό οικονομικό κλίμα μπορεί να έχει σημαντική επίδραση στην κεφαλαιοποίηση της αγοράς ενός κρυπτονομίσματος. Όταν η οικονομία είναι σε καλή κατάσταση ή η αγορά βρίσκεται σε ανοδική πορεία, η κεφαλαιοποίηση τείνει να αυξάνεται. Αντίθετα, σε περιόδους οικονομικής ύφεσης ή πτωτικής αγοράς, η κεφαλαιοποίηση μπορεί να μειωθεί. Επιπλέον, η

υιοθέτηση των ψηφιακών νομισμάτων από μεγάλους θεσμικούς επενδυτές και χρηματοπιστωτικούς οργανισμούς αποτελεί έναν άλλο σημαντικό παράγοντα που επηρεάζει το μερίδιο αγοράς τους. Η συμμετοχή θεσμικών παραγόντων, όπως επενδυτικά κεφάλαια και τράπεζες, έχει οδηγήσει σε αύξηση της ζήτησης, ενισχύοντας παράλληλα τη θέση των πιο καθιερωμένων κρυπτονομισμάτων στην αγορά.

Παράλληλα, η εξέλιξη χρηματοπιστωτικών προϊόντων που συνδέονται με τα κρυπτονομίσματα, όπως τα ETFs (Exchange Traded Funds) και τα παράγωγα, έχει καταστήσει ευκολότερη την πρόσβαση των θεσμικών επενδυτών στην αγορά. Αυτό οδήγησε σε αύξηση του μεριδίου αγοράς των ψηφιακών νομισμάτων, ενισχύοντας τη σταθερότητά τους και προωθώντας την ευρύτερη αποδοχή τους ως επενδυτικά μέσα.

Ανταγωνισμός μεταξύ Δικτύων (Πλατφόρμων)

Ένας άλλος σημαντικός παράγοντας είναι ο ανταγωνισμός ανάμεσα στα διάφορα δίκτυα και πλατφόρμες κρυπτονομισμάτων. Κάθε πλατφόρμα επιδιώκει να ξεχωρίσει προσφέροντας μοναδικά χαρακτηριστικά, όπως αυξημένη ταχύτητα συναλλαγών, υποστήριξη έξυπνων συμβολαίων ή την ικανότητα διαχείρισης μεγάλου όγκου συναλλαγών. Χαρακτηριστικό παράδειγμα αποτελεί το Ethereum, το οποίο έχει καθιερωθεί ως η κύρια πλατφόρμα για έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές, βρίσκεται αντιμέτωπο με αυξανόμενο ανταγωνισμό από νεότερες πλατφόρμες όπως το Solana, που προσφέρει υψηλότερες ταχύτητες και χαμηλότερα κόστη. Αυτή η συνεχής προσπάθεια για τεχνολογική υπεροχή επηρεάζει άμεσα το μερίδιο αγοράς, καθώς οι χρήστες και οι προγραμματιστές στρέφονται προς τις πλατφόρμες που παρέχουν τις βέλτιστες λύσεις για τις ανάγκες τους.

Μέσα Ενημέρωσης

Οι επιδράσεις των μέσων ενημέρωσης στη διαμόρφωση της δημόσιας γνώμης αποτελούν έναν σημαντικό παράγοντα στην αλληλεπίδραση των κοινωνικών δυνάμεων που επηρεάζουν την αγορά των κρυπτονομισμάτων. Μέσω της μαζικής επικοινωνίας, όπως οι εφημερίδες, το ραδιόφωνο, η τηλεόραση, καθώς και οι σύγχρονες τεχνολογίες διαδικτύου και κινητών τηλεφώνων, μεταδίδονται πληροφορίες στο κοινό, διαμορφώνοντας έτσι τις αντιλήψεις του. Τα μέσα ενημέρωσης έχουν τη δύναμη όχι μόνο να υποδεικνύουν στο κοινό ποια θέματα πρέπει να προσέχει, αλλά και να διαμορφώνουν τον τρόπο σκέψης τους και τις αντίστοιχες δράσεις τους.

Η Tsvetkova, ο Yasserri, ο Meyer και οι συνεργάτες τους (2017) διερεύνησαν τις αλληλεπιδράσεις μεταξύ ανθρώπων και μηχανών στις αγορές προβλέψεων, καταλήγοντας στο συμπέρασμα ότι η ποιότητα της πληροφόρησης και η εμπιστοσύνη αποτελούν κρίσιμους παράγοντες που επηρεάζουν την κεφαλαιοποίηση της αγοράς και την εμπιστοσύνη των χρηστών σε αυτές τις πλατφόρμες. Τέλος, οι Li και Wang (2017) πρότειναν ότι θα μπορούσαν να υπάρχουν παράγοντες που σχετίζονται με τα συναισθήματα στα μέσα κοινωνικής δικτύωσης, τα οποία με τη σειρά τους μπορεί να συσχετίζονται με την αστάθεια των κρυπτονομισμάτων.

Κοινωνικοί Παράγοντες (Συναίσθημα της Αγοράς)

Το συναίσθημα της αγοράς, επηρεαζόμενο από κοινωνικούς παράγοντες, παίζει καθοριστικό ρόλο στη διαμόρφωση της ζήτησης για κρυπτονομίσματα. Η αποδοχή από μεγάλους θεσμικούς παράγοντες και οι θετικές ειδήσεις μπορούν να βελτιώσουν το κλίμα στην αγορά, αυξάνοντας τη ζήτηση για ένα κρυπτονόμισμα, κάτι που οδηγεί σε άνοδο των τιμών και, κατά συνέπεια, σε μεγαλύτερη κεφαλαιοποίηση. Αντίθετα, αρνητικές εξελίξεις, όπως παραβιάσεις ασφάλειας ή αυστηρές ρυθμιστικές παρεμβάσεις, μπορούν να κλονίσουν την εμπιστοσύνη των επενδυτών, προκαλώντας πτώση τόσο στις τιμές όσο και στην κεφαλαιοποίηση. Επομένως, η συνεχής παρακολούθηση των εξελίξεων και του κλίματος στην αγορά των κρυπτονομισμάτων είναι απαραίτητη πριν από κάθε επενδυτική κίνηση.

Επίσης, υπάρχουν συγκεκριμένοι κοινωνικοί παράγοντες που θεωρείται ότι επηρεάζουν την αγορά των ψηφιακών νομισμάτων, όπως είναι: οι ανακοινώσεις τραπεζών σχετικά με τα κρυπτονομίσματα, κυβερνητικές ρυθμίσεις, απόψεις γνωστών τεχνολογικών προσωπικοτήτων που σχετίζονται με τη βιομηχανία των κρυπτονομισμάτων, απόψεις δημοφιλών διασημοτήτων, ειδήσεις από ανταλλακτήρια κρυπτονομισμάτων, πληροφορίες που αφορούν απαγορεύσεις κρυπτονομισμάτων, ανακοινώσεις σχετικά με τα κρυπτονομίσματα από μεγάλες εταιρείες ή ρυθμιστικές αρχές και πληροφορίες για απάτες που σχετίζονται με κρυπτονομίσματα (Aggarwal, G. et al. (2019)).

Κατανοώντας λοιπόν τους παραπάνω παράγοντες, οι επενδυτές μπορούν να αποκτήσουν μια πιο βαθιά αντίληψη των δυνάμεων που επηρεάζουν την κεφαλαιοποίηση της αγοράς και να λάβουν πιο ενημερωμένες επενδυτικές αποφάσεις όσον αφορά τα κρυπτονομίσματα.

3.3. Επενδυτικές Στρατηγικές των Ψηφιακών Νομισμάτων

Οι επενδυτικές στρατηγικές στον χώρο των ψηφιακών νομισμάτων έχουν γίνει εξαιρετικά δημοφιλείς, καθώς η τεχνολογία Blockchain και η αυξανόμενη φήμη των κρυπτονομισμάτων δημιουργούν νέες ευκαιρίες για τους επενδυτές. Από τη μακροπρόθεσμη διακράτηση έως το Day Trading, οι επενδυτές υιοθετούν διαφορετικές προσεγγίσεις για να αξιοποιήσουν τις ευκαιρίες της αγοράς. Στη συνέχεια, θα εξετάσουμε κάποιες επενδυτικές στρατηγικές που έχουν αναπτυχθεί για τα ψηφιακά νομίσματα.

1. Μακροπρόθεσμη Επένδυση (HODL)

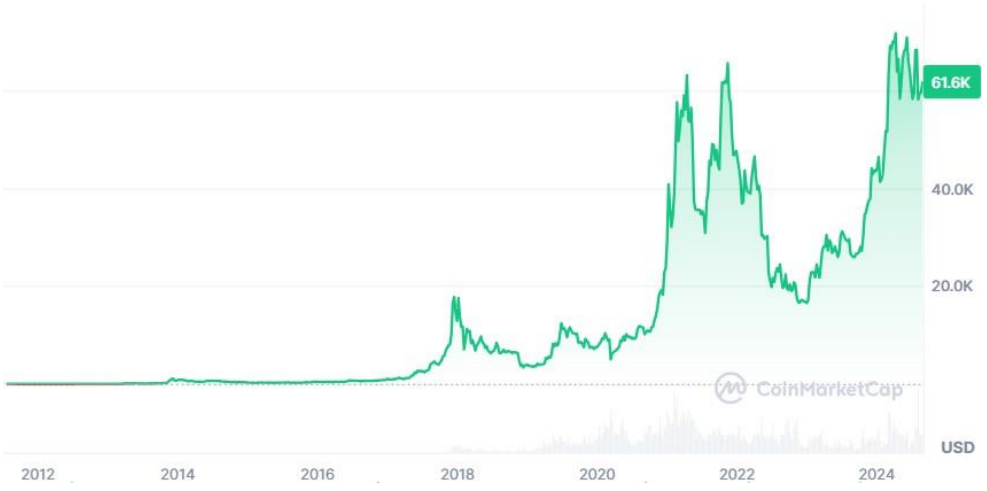
Μία από τις πιο διαδεδομένες και απλούστερες στρατηγικές στον κόσμο των κρυπτονομισμάτων είναι η μακροχρόνια επένδυση, γνωστή και ως "HODL". Η βασική ιδέα πίσω από αυτήν τη στρατηγική είναι να αγοράζεις όταν οι τιμές είναι χαμηλές και να πουλάς όταν οι τιμές αυξηθούν σημαντικά.

Ο όρος "HODL" προέκυψε το 2013 από ένα τυπογραφικό λάθος της λέξης "hold" σε μια ανάρτηση στο φόρουμ Bitcointalk. Παρά το λάθος, ο όρος έγινε δημοφιλής και πλέον αντιπροσωπεύει τη στρατηγική της διατήρησης ενός κρυπτονομίσματος για μεγάλο χρονικό διάστημα, ανεξαρτήτως των βραχυπρόθεσμων διακυμάνσεων της τιμής του. Συγκεκριμένα, την εποχή εκείνη, η τιμή του Bitcoin ήταν εξαιρετικά ασταθής, σημειώνοντας απότομη άνοδο από περίπου 130 δολάρια τον Απρίλιο του 2013 σε πάνω από 950 δολάρια τον Δεκέμβριο του ίδιου έτους. Ο χρήστης που είχε κάνει την ανάρτηση ενθάρρυνε τους άλλους επενδυτές να μη πουλήσουν τα νομίσματά τους, δηλώνοντας ότι ο ίδιος "hodling". Έκτοτε, το "HODL"

χρησιμοποιείται για να περιγράψει τη στρατηγική της αγοράς και διακράτησης (buy and hold) ψηφιακών νομισμάτων με στόχο την επίτευξη κέρδους σε μακροπρόθεσμη βάση, παραβλέποντας τις βραχυχρόνιες διακυμάνσεις των τιμών.

Οι επενδυτές που επιλέγουν να ακολουθήσουν αυτή τη στρατηγική συνήθως πιστεύουν ότι η τεχνολογία blockchain θα συνεχίσει να αναπτύσσεται και ότι τα κρυπτονομίσματα θα αποκτήσουν μεγαλύτερη αξία με την πάροδο του χρόνου. Αυτοί οι επενδυτές θεωρούν ότι οι βραχυπρόθεσμες διακυμάνσεις των τιμών δεν είναι παρά προσωρινές διαταραχές και ότι η πραγματική αξία των κρυπτονομισμάτων θα αναδειχθεί σε μακροπρόθεσμη βάση. Παρ' όλα αυτά, η στρατηγική HODL απαιτεί από τους επενδυτές να έχουν υπομονή και να αντέχουν τους κινδύνους, καθώς η αγορά κρυπτονομισμάτων είναι γνωστή για την έντονη αστάθεια της.

Για παράδειγμα, αν κάποιος είχε υιοθετήσει τη στρατηγική HODL και είχε αγοράσει Bitcoin σε πρώιμα στάδια, για παράδειγμα το 2012 ή 2013 όταν η τιμή ήταν πολύ χαμηλή, θα είχε δει σημαντική αύξηση της αξίας της επένδυσής του μέχρι το 2024, όπως φαίνεται στο Γράφημα (Εικόνα 8). Παρά τις έντονες διακυμάνσεις και τις απότομες πτώσεις κατά την πορεία της τιμής, η στρατηγική θα είχε αποδώσει εξαιρετικά, με την τιμή του Bitcoin να φτάνει πάνω από 61.000 δολάρια. Αυτό επιβεβαιώνει την κεντρική ιδέα της στρατηγικής HODL, ότι η μακροχρόνια διακράτηση ενός ψηφιακού νομίσματος μπορεί να αποφέρει σημαντικά κέρδη, παρά τις βραχυπρόθεσμες διακυμάνσεις στην αγορά.



Εικόνα 8. Ιστορική εξέλιξη της τιμής του Bitcoin (2012-2024) σε USD (Πηγή: CoinMarketCap.com).

2. Ημερήσια διαπραγμάτευση (Day Trading)

Αντίθετα από τη στρατηγική HODL, η οποία επικεντρώνεται στη μακροπρόθεσμη διακράτηση κρυπτονομισμάτων, η ημερήσια διαπραγμάτευση δίνει έμφαση στη βραχυπρόθεσμη κερδοσκοπία. Οι day traders, για παράδειγμα, προσπαθούν να εκμεταλλευτούν τις καθημερινές διακυμάνσεις της τιμής, αγοράζοντας και πουλώντας ψηφιακά νομίσματα με στόχο την αποκόμιση μικρών αλλά συχνών κερδών από τις διαφορές στην τιμή.

Για την επιτυχία σε αυτή τη στρατηγική, είναι απαραίτητη η κατανόηση των αγορών και η ικανότητα εφαρμογής της τεχνικής και θεμελιώδους ανάλυσης. Επιπλέον, οι traders συχνά καταφεύγουν στη χρήση αυτοματοποιημένων εργαλείων και bots για την εκτέλεση συναλλαγών, προκειμένου να αξιοποιήσουν κάθε ευκαιρία που παρουσιάζεται. Παρά τα πιθανά οφέλη, η στρατηγική αυτή συνοδεύεται από υψηλό κίνδυνο, καθώς οι τιμές μπορεί να μεταβάλλονται απότομα και απρόβλεπτα.

Ενεργές στρατηγικές ημερήσιας διαπραγμάτευσης, όπως το day trading και το swing trading, αποτελούν κοινές πρακτικές στις αγορές κρυπτονομισμάτων, καθώς προσφέρουν στους επενδυτές τη δυνατότητα να αξιοποιήσουν τη μεταβλητότητα των τιμών μέσα από συχνές συναλλαγές.

3. Στρατηγική Staking

Το Staking αποτελεί μια δημοφιλή στρατηγική που επιτρέπει στους επενδυτές να κερδίζουν παθητικά εισοδήματα, λαμβάνοντας μέρος στη διαδικασία επικύρωσης συναλλαγών σε δίκτυα που βασίζονται στον μηχανισμό PoS. Πιο συγκεκριμένα, οι επενδυτές "κλειδώνουν" τα νομίσματά τους σε ένα συγκεκριμένο πορτοφόλι και, σε αντάλλαγμα, λαμβάνουν ανταμοιβές με τη μορφή επιπλέον κρυπτονομισμάτων. Αυτή η στρατηγική είναι ιδιαίτερα ελκυστική για όσους θέλουν να απολαμβάνουν σταθερά έσοδα χωρίς να χρειάζεται να πωλήσουν τα ψηφιακά τους νομίσματα. Είναι μια λιγότερο ενεργή αλλά δυνητικά αποδοτική προσέγγιση, ειδικά αν οι επενδυτές πιστεύουν στη μακροπρόθεσμη προοπτική του κρυπτονομίσματος που έχουν επιλέξει.

Ωστόσο, είναι σημαντικό να γίνεται προσεκτική επιλογή του κατάλληλου δικτύου, καθώς οι αποδόσεις μπορούν να επηρεαστούν τόσο από την αστάθεια της αγοράς όσο και από τις αλλαγές στους κανονισμούς. Συμμετέχοντας σε δίκτυα PoS, οι επενδυτές μπορούν να ενισχύσουν τα παθητικά τους έσοδα, ενσωματώνοντας αυτήν τη στρατηγική στο συνολικό επενδυτικό τους σχέδιο, λαμβάνοντας υπόψη τις προκλήσεις και τις δυνατότητες που προσφέρει.

4. Τεχνική Ανάλυση (Technical Analysis)

Μια ευρέως χρησιμοποιούμενη στρατηγική τόσο στις παραδοσιακές αγορές όσο και στις αγορές κρυπτονομισμάτων είναι η τεχνική ανάλυση. Αυτή η μέθοδος στηρίζεται στην ανάλυση ιστορικών τιμών και μοτίβων στις συναλλαγές για την πρόβλεψη των μελλοντικών κινήσεων της αγοράς. Οι επενδυτές που την εφαρμόζουν, μελετούν διαγράμματα τιμών, όγκους συναλλαγών, και διάφορους τεχνικούς δείκτες, όπως οι κινητοί μέσοι όροι. Θα λέγαμε ότι, αποδεικνύεται ιδιαίτερα χρήσιμη για βραχυπρόθεσμες συναλλαγές, καθώς παρέχει στους επενδυτές τα εργαλεία για να αποφασίσουν πότε να εισέλθουν ή να αποχωρήσουν από την αγορά.

5. Θεμελιώδης Ανάλυση (Fundamental Analysis)

Η θεμελιώδης ανάλυση, σε αντίθεση με την τεχνική ανάλυση που αναφέραμε προηγουμένως, εστιάζει στη μελέτη των βασικών παραγόντων που επηρεάζουν την αξία ενός κρυπτονομίσματος. Οι επενδυτές που την εφαρμόζουν, επικεντρώνονται στην αξιολόγηση της ομάδας που αναπτύσσει το νόμισμα, το επίπεδο αποδοχής και υιοθέτησης της τεχνολογίας του, καθώς και τη δύναμη της κοινότητας που το στηρίζει.

Αυτή η προσέγγιση επιτρέπει στους επενδυτές να εντοπίζουν ποια ψηφιακά νομίσματα έχουν τις μεγαλύτερες προοπτικές μακροπρόθεσμης επιτυχίας, βοηθώντας τους να λάβουν αποφάσεις για τις επενδύσεις τους με γνώμονα το μέλλον. Παρότι η θεμελιώδης ανάλυση μπορεί να μην προσφέρει άμεσα κέρδη, μπορεί να οδηγήσει σε σημαντικές αποδόσεις για εκείνους που κάνουν σωστές επιλογές.

6. Στρατηγική Dollar-Cost Averaging (DCA)

Η στρατηγική DCA είναι μια από τις πιο δημοφιλείς επιλογές για νέους επενδυτές στον κόσμο των κρυπτονομισμάτων, καθώς προσφέρει μια σταθερή και μεθοδική προσέγγιση στην επένδυση. Εφαρμόζοντας αυτήν τη στρατηγική, οι επενδυτές δεσμεύονται να επενδύουν ένα συγκεκριμένο ποσό σε τακτά χρονικά διαστήματα, ανεξάρτητα από την τρέχουσα τιμή του κρυπτονομίσματος. Με αυτόν τον τρόπο, αποφεύγουν τον κίνδυνο να τοποθετήσουν όλα τα κεφάλαιά τους σε μια περίοδο κατά την οποία οι τιμές είναι υψηλές, μειώνοντας έτσι την πιθανότητα να αγοράσουν σε ακατάλληλες χρονικές στιγμές.

Επιπλέον, αυτή η μέθοδος είναι ιδιαίτερα χρήσιμη για εκείνους που δεν έχουν την εμπειρία ή τον χρόνο να παρακολουθούν συνεχώς τις αγορές, διότι μπορούν να οικοδομήσουν το χαρτοφυλάκιό τους σταδιακά, με λιγότερο άγχος και μεγαλύτερη ηρεμία. Η στρατηγική DCA προσφέρει έτσι μια απλή αλλά αποτελεσματική προσέγγιση για τη μακροπρόθεσμη ανάπτυξη των επενδύσεων, εξομαλύνοντας τις επιπτώσεις της αγοράς και εξασφαλίζοντας ότι οι επενδύσεις τους πραγματοποιούνται με συνέπεια και σταθερότητα.

7. Στρατηγική Arbitrage

Βασίζεται στην εκμετάλλευση των διαφορών στις τιμές ενός κρυπτονομίσματος μεταξύ διαφορετικών ανταλλακτηρίων. Οι επενδυτές που ακολουθούν αυτήν τη στρατηγική αγοράζουν το κρυπτονόμισμα από το ανταλλακτήριο με την χαμηλότερη τιμή και το πωλούν σε άλλο ανταλλακτήριο όπου η τιμή είναι υψηλότερη, αποκομίζοντας έτσι κέρδη από τη διαφορά. Ωστόσο, αν και η στρατηγική μπορεί να φαίνεται απλή στη θεωρία, η εφαρμογή της στην πράξη παρουσιάζει προκλήσεις, καθώς ο χρόνος είναι κρίσιμος και οι συναλλαγές πρέπει να εκτελεστούν γρήγορα, ενώ οι προμήθειες των ανταλλακτηρίων μπορούν επίσης να μειώσουν σημαντικά τα κέρδη, καθιστώντας τη στρατηγική λιγότερο αποδοτική.

Στο δυναμικό περιβάλλον των κρυπτονομισμάτων, αυτή η στρατηγική απαιτεί όχι μόνο ταχύτητα, αλλά και την ικανότητα να εντοπίζονται γρήγορα οι διαφορές τιμών μεταξύ των ανταλλακτηρίων. Όσοι μπορούν να αντιδράσουν άμεσα και να εκμεταλλευτούν αυτές τις ευκαιρίες, έχουν τη δυνατότητα να αποκομίσουν σημαντικά κέρδη, αλλά πρέπει να είναι πάντα προσεκτικοί λόγω των κινδύνων που ελλοχεύουν.

Συνοψίζοντας, οι επενδυτικές στρατηγικές στον τομέα των ψηφιακών νομισμάτων προσφέρουν μια ευρεία γκάμα ευκαιριών, αλλά ταυτόχρονα συνοδεύονται από σημαντικές προκλήσεις που απαιτούν σκέψη και προετοιμασία. Η εις βάθος κατανόηση των διαφορετικών στρατηγικών και η συνεχής ενημέρωση είναι καθοριστικής σημασίας για τη λήψη αποφάσεων και την αποτελεσματική πλοήγηση στον δυναμικό κόσμο των κρυπτονομισμάτων.

Οι επενδυτές καλούνται να επιλέξουν τη στρατηγική που εναρμονίζεται με τους προσωπικούς τους στόχους, το επίπεδο ανοχής τους στον κίνδυνο και τον επενδυτικό τους ορίζοντα. Εκείνοι που διαθέτουν την ικανότητα να προσαρμόζουν τις στρατηγικές τους στις διαρκώς μεταβαλλόμενες συνθήκες της αγοράς θα μπορέσουν να αξιοποιήσουν τις ευκαιρίες που θα προκύψουν, καθώς ο τομέας των ψηφιακών νομισμάτων συνεχίζει να εξελίσσεται και να αναπτύσσεται με ραγδαίο ρυθμό.

3.4. Μελλοντικό Μερίδιο Αγοράς

Η αγορά των ψηφιακών νομισμάτων έχει εξελιχθεί ραγδαία την τελευταία δεκαετία, με την κεφαλαιοποίηση της αγοράς να σημειώνει εντυπωσιακές αυξήσεις, αλλά και σημαντικές διακυμάνσεις. Οι προβλέψεις για το μελλοντικό μερίδιο αγοράς των ψηφιακών νομισμάτων αποτελούν αντικείμενο έντονης συζήτησης και ανάλυσης, καθώς επηρεάζονται από μια σειρά παραγόντων, όπως οι τεχνολογικές εξελίξεις, οι κανονιστικές ρυθμίσεις, οι οικονομικές συνθήκες και η αποδοχή από το ευρύ κοινό.

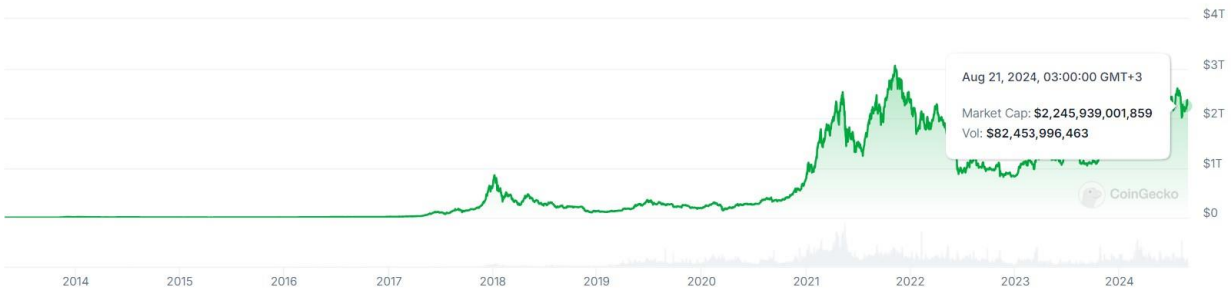
Ειδικότερα, όσο αφορά το Bitcoin, έχει δείξει συγκεκριμένα και επαναλαμβανόμενα μοτίβα τιμών, τα οποία ακολουθούν έναν κύκλο τεσσάρων ετών. Συγκεκριμένα, συνήθως παρατηρείται μια περίοδος πτωτικής αγοράς, όπως αυτή του 2022, ακολουθούμενη από μια σημαντική ανάκαμψη τον επόμενο χρόνο. Κατά τον τρίτο χρόνο, που είναι η χρονιά του halving, οι τιμές συχνά συνεχίζουν να αυξάνονται. Το halving είναι ένα γεγονός που συμβαίνει κάθε τέσσερα χρόνια, μειώνοντας τις ανταμοιβές ανά μπλοκ κατά 50%, κάτι που περιορίζει την προσφορά των νέων bitcoins και μπορεί να οδηγήσει σε αύξηση της τιμής, εφόσον οι συνθήκες της αγοράς παραμένουν αμετάβλητες. Συνήθως, ο κύκλος ολοκληρώνεται με μια κορύφωση την τέταρτη χρονιά μετά το halving.

Αυτή τη στιγμή, βρισκόμαστε στον τρίτο χρόνο αυτού του κύκλου, κατά την διάρκεια του halving, και το Bitcoin φαίνεται να ακολουθεί το παραδοσιακό τετραετές μοτίβο του. Παρόλο που η απόδοση του παρελθόντος δεν εγγυάται τις μελλοντικές εξελίξεις, τα ιστορικά δεδομένα μπορούν να προσφέρουν μια βάση για προσεκτικές προβλέψεις. Έτσι λοιπόν, ας εξετάσουμε το τετραετές μοντέλο για να αξιολογήσουμε την μελλοντική εξέλιξη του Bitcoin, λαμβάνοντας υπόψη τις τρέχουσες συνθήκες αγοράς.

Αρχικά, κατά τη διάρκεια του halving, το Bitcoin έχει παρουσιάσει κατά μέσο όρο αύξηση της τάξεως του 125%. Εάν αυτό το μοτίβο επαναληφθεί και φέτος, τότε θα μπορούσαμε να αναμένουμε ότι η τιμή του Bitcoin θα αγγίξει περίπου τα 100.000 δολάρια μέχρι το τέλος του 2024. Αυτή η πρόβλεψη βασίζεται σε μια αύξηση 125% από την αρχική τιμή του Bitcoin στις αρχές του έτους, η οποία ήταν στα 44.000 δολάρια (Πηγή: Yahoo Finance).

Από τα ιστορικά δεδομένα της τιμής του Bitcoin, παρατηρούμε ότι, παρουσιάζει μια εντυπωσιακή αύξηση της τάξης του 400%, μετά το halving. Η βασική αιτία για αυτή τη σημαντική άνοδο είναι ότι η αγορά αρχίζει να αντιλαμβάνεται τις επιπτώσεις του halving, με το σοκ στην προσφορά να γίνεται αισθητό. Εάν αυτό το μοτίβο επαναληφθεί και το Bitcoin κλείσει το 2024 σύμφωνα με τον ιστορικό μέσο όρο, τότε η τιμή του θα μπορούσε να φτάσει περίπου στα 500.000 δολάρια μέσα στο 2025. Παρ 'όλα αυτά, όσο απίστευτο κι αν ακούγεται αυτό το ποσό, το Bitcoin έχει επανειλημμένα υπερβεί τις προσδοκίες σε περιόδους ανοδικών αγορών, αποκτώντας φήμη για τέτοιου είδους επιδόσεις. Επομένως, ενώ τα 500.000 δολάρια μπορεί να φαίνονται υπερβολικά, έχουν συμβεί και πιο απρόβλεπτα γεγονότα, όπως για παράδειγμα, το 2011 που το κρυπτονόμισμα κατέγραψε αύξηση 850%.

Παρακάτω, στο γράφημα (Εικόνα 9) παρουσιάζεται η πορεία της συνολικής κεφαλαιοποίησης της αγοράς κρυπτονομισμάτων από τον Ιανουάριο του 2022 έως την 21η Αυγούστου του 2024, ενώ στο δεύτερο γράφημα (Εικόνα 10) δίνεται και μια πρόβλεψη για την εξέλιξή της μέχρι την 21η Αυγούστου του 2025. Βλέπουμε ότι, η τρέχουσα συνολική κεφαλαιοποίηση της αγοράς κρυπτονομισμάτων ανέρχεται περίπου στα 2.24 τρισεκατομμύρια δολάρια.



Εικόνα 9. Η συνολική κεφαλαιοποίηση και ο όγκος συναλλαγών των κρυπτονομισμάτων (2014-2024) (Πηγή: CoinGecko.com).

Σύμφωνα με την πρόβλεψη για την αντίστοιχη ημερομηνία το έτος 2025, εκτιμάται ότι η συνολική κεφαλαιοποίηση θα μειωθεί στα 2.03 τρισεκατομμύρια δολάρια, καταγράφοντας μια πτώση περίπου 9.38%, σε σχέση με την τρέχουσα τιμή. Παράλληλα, οι δείκτες συναισθήματος και φόβου/απληστίας βρίσκονται σε ουδέτερα επίπεδα, υποδηλώνοντας αβεβαιότητα στην αγορά.

Εικόνα 9. Τρέχουσα και μελλοντική συνολική κεφαλαιοποίηση της αγοράς των κρυπτονομισμάτων (2022-2025) (Πηγή: CoinCodex).

Συνοψίζοντας, η γενική εικόνα για το 2025 αρχικά δείχνει μια ανοδική τάση, συγκριτικά με τα προηγούμενα έτη. Ωστόσο, κατά τους καλοκαιρινούς μήνες (Ιούλιο-Αύγουστο), εμφανίζεται μια μεγαλύτερη πτώση σε σχέση με τους αντίστοιχους μήνες του 2024, καταλήγοντας σε χαμηλότερα επίπεδα κεφαλαιοποίησης. Αυτή η διακύμανση στην αγορά των κρυπτονομισμάτων υποδηλώνει ότι, παρά τη δυναμική φύση της αγοράς, η τρέχουσα κεφαλαιοποίηση μειώνεται ελαφρώς, με τις προβλέψεις να δείχνουν περαιτέρω πτώση στο μέλλον για τους καλοκαιρινούς μήνες. Καθώς η αγορά παραμένει ιδιαίτερα ασταθής, οι επενδυτές θα πρέπει να παραμένουν ενημερωμένοι και να προσαρμόζουν τις στρατηγικές τους ανάλογα με τις μεταβαλλόμενες συνθήκες.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα ψηφιακά νομίσματα, ιδιαίτερα τα κρυπτονομίσματα, έχουν εξελιχθεί σημαντικά την τελευταία δεκαετία, ενώ παράλληλα παραμένουν στο επίκεντρο συζητήσεων σε θέματα ρύθμισης και οικονομικής πολιτικής παγκοσμίως. Σε αντίθεση με τις τράπεζες, προσφέρουν ταχύτητα, ασφάλεια και μειωμένο κόστος στις συναλλαγές, καθιστώντας τα πιο προσβάσιμα, ιδιαίτερα σε άτομα που δεν έχουν πρόσβαση σε παραδοσιακές τραπεζικές υπηρεσίες.
Επιπλέον, η αγορά των κρυπτονομισμάτων αποτελεί έναν δυναμικό και συνεχώς εξελισσόμενο τομέα, χαρακτηριζόμενο από υψηλή μεταβλητότητα. Οι τεχνολογικές εξελίξεις, οι ρυθμιστικές παρεμβάσεις και το γενικότερο οικονομικό κλίμα διαδραματίζουν καθοριστικό ρόλο στην πορεία των κρυπτονομισμάτων. Παράλληλα, το συναίσθημα των επενδυτών, το οποίο διαμορφώνεται από τις ειδήσεις και τα μέσα ενημέρωσης, παίζει επίσης σημαντικό ρόλο στις διακυμάνσεις των τιμών των κρυπτονομισμάτων, με τις ανακοινώσεις τραπεζών, τις ρυθμιστικές αλλαγές και τις απόψεις των τεχνολογικών προσωπικοτήτων να έχουν τη δύναμη να επηρεάζουν σημαντικά τις αγορές. Επιπρόσθετα, η αγορά των ψηφιακών νομισμάτων προσφέρει μια ποικιλία επενδυτικών στρατηγικών, από τη μακροπρόθεσμη διακράτηση μέχρι την ημερήσια διαπραγμάτευση και το staking. Συνεπώς, η κατανόηση και η προσαρμογή αυτών των στρατηγικών στις διαρκώς μεταβαλλόμενες συνθήκες της αγοράς είναι κρίσιμη για την επιτυχή επένδυση στον τομέα αυτόν.

Παρά τις αισιόδοξες προβλέψεις για την άνοδο της τιμής του Bitcoin, με εκτιμήσεις ότι μπορεί να φτάσει τα 500.000 δολάρια μέχρι το 2025, αναμένεται ότι η συνολική κεφαλαιοποίηση της αγοράς των κρυπτονομισμάτων μπορεί να υποστεί ελαφρά μείωση, φτάνοντας τα 2.03 τρισεκατομμύρια δολάρια. Αυτό υποδεικνύει ότι, ενώ κάποια νομίσματα μπορεί να αυξήσουν την αξία τους, η συνολική αγορά ενδέχεται να αντιμετωπίσει πιέσεις.

Συμπερασματικά, το μέλλον των ψηφιακών νομισμάτων παραμένει αβέβαιο, αλλά η αυξανόμενη αποδοχή τους από μεγάλες επιχειρήσεις και οργανισμούς, καθώς και η ανάπτυξη νέων τεχνολογιών και ρυθμιστικών πλαισίων, δείχνουν ότι τα ψηφιακά νομίσματα θα συνεχίσουν να διαδραματίζουν σημαντικό ρόλο στην παγκόσμια οικονομία. Ωστόσο, η εξέλιξή τους θα εξαρτηθεί από το πώς θα αντιμετωπιστούν οι προκλήσεις που ανακύπτουν, όπως η ρύθμιση, η ασφάλεια και η προστασία των δεδομένων, καθώς και από το πώς οι κυβερνήσεις και οι οργανισμοί θα επιλέξουν να προσαρμοστούν στη νέα αυτή πραγματικότητα.

ΜΕΘΟΔΟΛΟΓΙΑ PRISMA

Πρωτόκολλο και καταγραφή

Για τη διεξαγωγή της παρούσας έρευνας σχετικά με τα ψηφιακά νομίσματα και την τεχνολογία Blockchain, ακολουθήθηκε το πρωτόκολλο PRISMA 2020 (Page et al., 2021). Αυτή η μεθοδολογία καθορίζει σαφώς την πολιτική αναζήτησης, τα κριτήρια επιλογής των δημοσιεύσεων που θα συμπεριληφθούν στην ανασκόπηση, καθώς και τα κριτήρια απόρριψης, ενώ παράλληλα κατευθύνει τη διαδικασία εξαγωγής δεδομένων από τα ερευνητικά άρθρα.

Κριτήρια ένταξης μελετών

Για τη συλλογή ερευνητικών εργασιών και άρθρων και την εξέταση των εξελίξεων και ευρημάτων στο συγκεκριμένο πεδίο, ο σκοπός της παρούσας μελέτης είναι να ανασκοπήσει συστηματικά τις υπάρχουσες δημοσιεύσεις που αφορούν τα ψηφιακά νομίσματα και την τεχνολογία Blockchain.

Για την επίτευξη του σκοπού αυτού, τα χαρακτηριστικά των μελετών που ανασκοπήθηκαν ήταν τα εξής:

- Συμπεριλήφθηκαν μόνο δημοσιεύσεις στην αγγλική γλώσσα
- Η ανασκόπηση επικεντρώθηκε σε μελέτες που δημοσιεύτηκαν μετά το 2008
- Επιλέχθηκαν μελέτες που έχουν δημοσιευθεί σε επιστημονικά περιοδικά (peer-reviewed), άρθρα, διπλωματικές διατριβές αλλά και μελέτες από επιστημονικά συνέδρια

Πηγές πληροφοριών

Μια αναζήτηση βιβλιογραφίας πραγματοποιήθηκε στις βάσεις δεδομένων Google Scholar, Science Direct και Springer Link, αλλά και από ιστοσελίδες όπως Yahoo Finance, CoinMarketCap και CoinGecko.

Βιβλιογραφική αναζήτηση

Για την αναζήτηση χρησιμοποιήθηκαν συγκεκριμένες λέξεις-κλειδιά που σχετίζονται με τα ψηφιακά νομίσματα και την τεχνολογία Blockchain, όπως "digital currency", "cryptocurrency", "blockchain", "Bitcoin", και "financial technology", "market capitalizatioin".

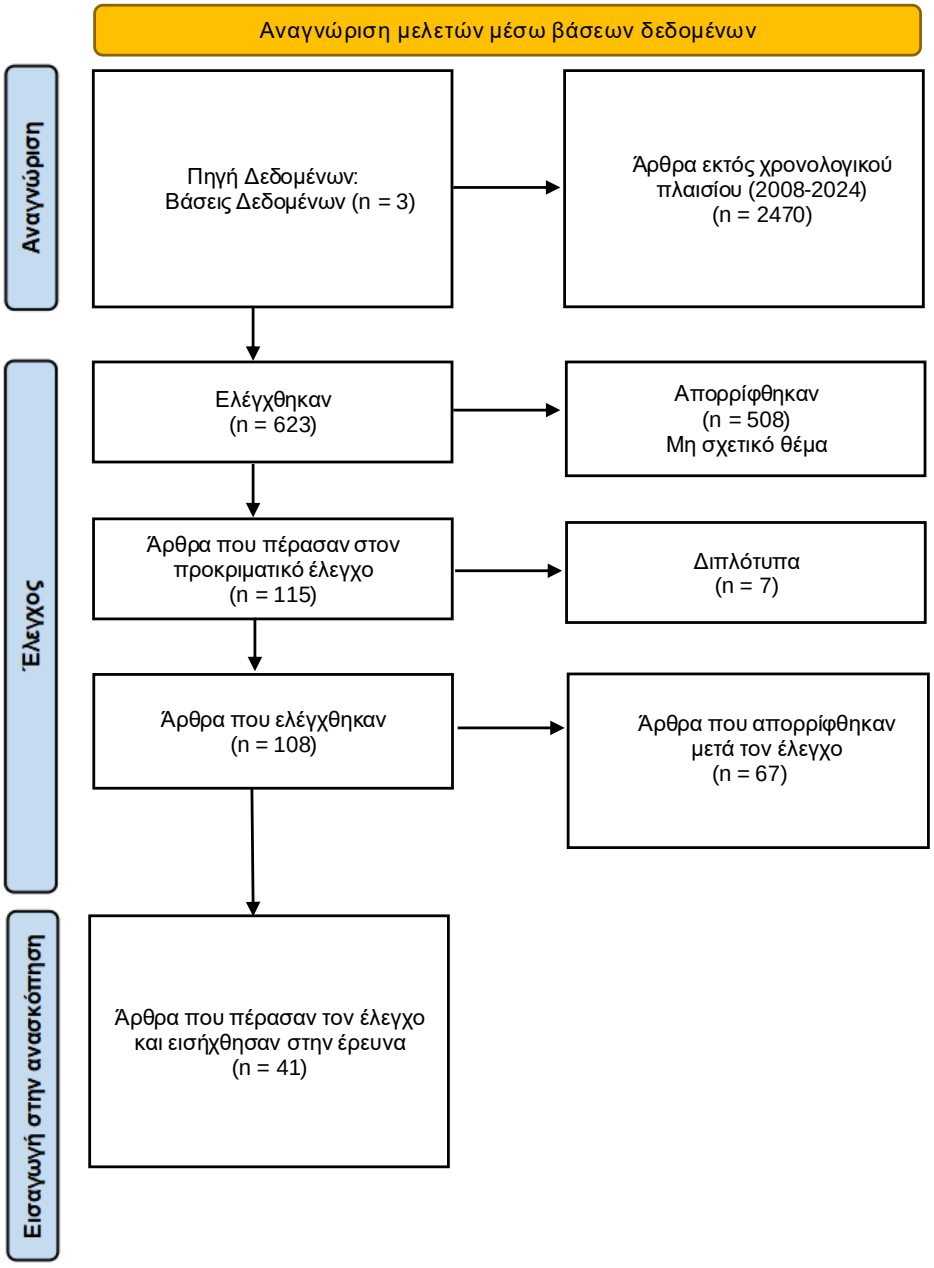
Διαδικασία επιλογής μελετών

Συγκεκριμένα, η αναζήτηση στη βάση δεδομένων Google Scholar πραγματοποιήθηκε με τις λέξεις κλειδιά "digital currency", "cryptocurrency", "Bitcoin", "blockchain", "market capitalizatioin" και έδωσε πάνω από 300.000 αποτελέσματα. Στη βάση δεδομένων Science Direct, η αναζήτηση ήταν πιο στοχευμένη, κάνοντας χρήση διαφόρων φίλτρων (όπως επιλογή θεματικής περιοχής, είδος άρθρου κ.α.), επιστρέφοντας 426 αποτελέσματα. Τέλος, στη βάση δεδομένων Springer Link η αναζήτηση επέστρεψε συνολικά 7.867 αποτελέσματα.

Είναι προφανές ότι δεν είναι εφικτό να συμπεριληφθούν όλα τα αποτελέσματα σε αυτήν τη διπλωματική εργασία. Για τον λόγο αυτό, εφαρμόστηκε ένας αρχικός έλεγχος με σκοπό τον εντοπισμό των σχετικών άρθρων. Στη συνέχεια, εξετάστηκε ο τίτλος κάθε άρθρου για να διαπιστωθεί αν είναι σύμφωνος με τις φράσεις και τις λέξεις-κλειδιά που αναφέρθηκαν προηγουμένως.

Στην αρχική φάση της έρευνας, από τη μηχανή αναζήτησης Google Scholar επιλέχθηκαν συνολικά 76 άρθρα και μελέτες, τα οποία προωθήθηκαν για προκαταρκτική αξιολόγηση. Από την πλατφόρμα Science Direct επιλέχθηκαν επιπλέον 12 άρθρα, ενώ από την Springer Link προστέθηκαν ακόμα 27. Όλα αυτά τα επιλεγμένα άρθρα προχώρησαν στη φάση του προκριματικού ελέγχου, όπου αξιολογήθηκε η καταλληλότητά τους με βάση τις αρχικές περιλήψεις τους. Τελικά, τα άρθρα τα οποία εισήχθησαν στην έρευνα είναι 41.

Ακολουθώντας τη μεθοδολογία PRISMA, παρουσιάζεται παρακάτω το διάγραμμα ροής της έρευνας.


Αναγνώριση μελετών μέσω βάσεων δεδομένων
Αναγνώριση
Πηγή Δεδομένων:
Βάσεις Δεδομένων (n = 3)
Άρθρα εκτός χρονολογικού πλαισίου (2008-2024)
(n = 2470)
Έλεγχος
Ελέγχθηκαν
(n = 623)
Απορρίφθηκαν
(n = 508)
Μη σχετικό θέμα
Άρθρα που πέρασαν στον προκριματικό έλεγχο
(n = 115)
Διπλότυπα
(n = 7)
Άρθρα που ελέγχθηκαν
(n = 108)
Άρθρα που απορρίφθηκαν μετά τον έλεγχο
(n = 67)
Εισαγωγή στην ανασκόπηση
Άρθρα που πέρασαν τον έλεγχο και εισήχθησαν στην έρευνα
(n = 41)

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Accenture Research. (2017). The (R)evolution of Money | Accenture.

[2] Adhami, S., Giudici, G. and Martinazzi, S. (2018). *Why do businesses go crypto? An empirical analysis of initial coin offerings*. Journal of Economics and Business, Volume 100, Pages 64-75, ISSN 0148-6195. https://doi.org/10.1016/j.jeconbus.2018.04.001

[3] Aggarwal, S. and Kumar, N. (2021). *Chapter Four - Digital signatures*. Cryptographic primitives used in blockchain, Advances in Computers, Elsevier, Volume 121, Pages 95-107, ISSN 0065-2458, ISBN 9780128219911. https://doi.org/10.1016/bs.adcom.2020.08.004

[4] Aggarwal, G. et al. (2019). *Understanding the Social Factors Affecting the Cryptocurrency Market.*

[5] Balcilar, M., Bouri, E., Gupta, R., Roubaud, D. (2017). Can volume predict Bitcoin returns and volatility? A quantiles-based approach. Economic Modelling 64, 74-81. ISSN 0264-9993. https://doi.org/10.1016/j. econmod.2017.03.019

[6] Buterin, V. (2014). *A next-generation smart contract and decentralized application platform.*

[7] Buterin, V. (7th August 2015). *On Public and Private Blockchains*. Ethereum Blog, Crypto Renaissance Salon.

[8] Campino, J., Brochado, A. & Rosa, Á. (2022). *Initial coin offerings (ICOs): Why do they succeed?*. Financ Innov 8, 17. https://doi.org/10.1186/s40854-021-00317-2

[9] D. Lee Kuo Chuen, Ed., *Handbook of Digital Currency*, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[10] Dr. Hariharan Narayanan (2020). *IS FUTURE A RULE OF DIGITAL CURRENCY???*. International Journal of Research - GRANTHAALAYAH, 8(8), 96-106. https://doi.org/10.29121/granthaalayah.v8.i8.2020.935

[11] Engert, W. and Fung, B. (2017). *Central Bank digital currency: Motivations and implications. Bank of Canada*. Staff Discussion Paper No. 2017-16. https://doi.org/10.34989/sdp-2017-16

[12] Giudici, G. and Rossi-Lamastra, C. (April 2018). *Crowdfunding of SMEs and Startups: When Open Investing Follows Open Innovation. Researching Open Innovation in SMEs*. Chapter 12, 377-396. https://doi.org/10.1142/9789813230972_0012

[13] Imogen, V. (2024). *A STUDY ON DIGITAL SIGNATURE IN BLOCKCHAIN TECHNOLOGY*.

[14] King, S. (July 7th, 2013). *Primecoin: Cryptocurrency with prime number proof-of-work.*

[15] King, S. and Nadal, S. (August 2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake*. Self-Published Paper, vol. 19.

[16] Li, Q., & Clark, G. (2013). *Mobile security: a look ahead*. IEEE Security & Privacy, 11(1), 78-81. https://doi.org/10.1109/MSP.2013.15

[17] Lim, J. W. (2015). *A Facilitative Model for Cryptocurrency Regulation in Singapore*. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, 361–381.https://doi.org/10.1016/B978-0-12-802117-0.00018-7

[18] Li., X. & Wang, C. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems 95, 49-60. ISSN 0167-9236. https://doi.org/10.1016/j.dss.2016.12.001

[19] Linuma, A. (2018). Why Is the Cryptocurrency Market So Volatile. (Online). https://cointelegraph.com/news/why-is-the-cryptocurrency-market-so-volatile-expert-take

[20] Maire, B. Le, Landau, E. J., & Genais, A. (June 2019). *Digital Currencies - An exploration into technology and money*.

[21] Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). *BYOD: Security and privacy considerations*. It Professional, 14(5), 53-55. https://doi.org/10.1109/MITP.2012.93

[22] Mullan, P.C. (2014). *What Is Digital Currency?*. In: The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations. Palgrave Pivot, New York. https://doi.org/10.1057/9781137382559_2

[23] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[24] Nalayini, C. M., Jeevaakatiravan, Imogen, P. V. and Sahana, J. M. (2023). *A Study on Digital Signature in Blockchain Technology*. Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, pp. 398-403. https://doi.org/10.1109/ICAIS56108.2023.10073680

[25] NRI (2015). *Survey on blockchain technologies and related services*. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

[26] Nurul, H., Nishchay, J. & Vinay, C. (2018). *BLOCKCHAIN, CRYPTOCURRENCY AND BITCOIN*.

[27] Peters, G. W., Panayi, E., & Chapelle, A. (2015). *Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective*. SSRN Electronic Journal, 3(3). https://doi.org/10.2139/ssrn.2646618

[28] Petrica, G., Axinte, S. D., Bacivarov, I. C., Firoiu, M., & Mihai, I. C. (2017). *Studying cyber security threats to web platforms using attack tree diagrams*. In Electronics, Computers and Artificial Intelligence (ECAI), 2017 9th International Conference on (pp. 1-6). https://doi.org/10.1109/ECAI.2017.8166456

[29] Priyadarshini, I. (2019). *Introduction to Blockchain Technology*. https://doi.org/10.1002/9781119488330

[30] Rose, C. (2015). *The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution*. International Business & Economics Research Journal (IBER), 14(4), 617. https://doi.org/10.19030/iber.v14i4.9353

[31] Seyed Mohammadreza Davoodalhosseini, (2022). *Central bank digital currency and monetary policy*. Journal of Economic Dynamics and Control. Volume 142, 104150, ISSN 0165-1889. https://doi.org/10.1016/j.jedc.2021.104150

[32] Shoaib, M., Ilyas M. and Hayat Khiyal M. S. (2013). *Official digital currency*. Eighth International Conference on Digital Information Management (ICDIM 2013), Islamabad, Pakistan. pp. 346-352. https://doi.org/10.1109/ICDIM.2013.6693982

[33] Singh, G., Garg, V., Tiwari, P. (2021). *Introduction to Blockchain Technology*. In: Agrawal, R., Gupta, N. (eds) Transforming Cybersecurity Solutions using Blockchain. Blockchain Technologies. Springer, Singapore. https://doi.org/10.1007/978-981-33-6858-3_1

[34] Skeie, David R. (December 1, 2021). *Digital Currency Runs*. WBS Finance Group Research Paper, Available at SSRN: https://ssrn.com/abstract=3294313 or http://dx.doi.org/10.2139/ssrn.3294313

[35] Subashini, S., & Kavitha, V. (2011). *A survey on security issues in service delivery models of cloud computing*. Journal of network and computer applications, 34(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[36] Taskinsoy, J. (October 13, 2021). *Bitcoin: A New Digital Gold Standard in the 21st Century?*. Available at SSRN: https://ssrn.com/abstract=3941857 or http://dx.doi.org/10.2139/ssrn.3941857

[37] Tsvetkova, M., Yasseri, T., Meyer, E. T., Pickering, J. B., Engen, V., Walland, P., Uders, M. Bravos, G. (2017). *Understanding human-machine networks: a cross-disciplinary survey*. ACM Computing Surveys (CSUR). 50(1), 12. https://arxiv.org/abs/1511.05324

[38] van Oorschot, P.C. (2021). *Bitcoin, Blockchains and Ethereum*. In: Computer Security and the Internet. Information Security and Cryptography. Springer, Cham. https://doi.org/10.1007/978-3-030-83411-1_13

[39] Vasin, P. (2014). *Blackcoins proof-of-stake protocol v2*. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[40] Wadsworth, A. (2018). *Bulletin - Reserve Bank of New Zealand*. 81(3), 1–14. https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin/2018/rbb2018-81-03

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