



ΑΡΙΣΤΟΤΕΛΕΙΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΘΕΣΣΑΛΟΝΙΚΗΣ

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

# ΑΝΑΠΤΥΞΗ ΑΛΓΟΡΙΘΜΟΥ ΣΤΑΘΕΡΟΥ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΟΣ ΧΩΡΙΣ ΑΝΑΓΚΗ ΕΝΕΧΥΡΟΥ ΦΥΣΙΚΟΥ ΝΟΜΙΣΜΑΤΟΣ

---

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΙΣΗΓΗΤΗΣ: ΑΛΕΞΑΝΔΡΟΣ ΤΣΙΡΩΝΗΣ 8258

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΑΝΔΡΕΑΣ ΣΥΜΕΩΝΙΔΗΣ

Θεσσαλονίκη, Μάρτιος 2022

## Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κύριο Ανδρέα Συμεωνίδη για την πολύ μεγάλη εμπιστοσύνη που μου έδειξε και την υποδειγματικότατη μεντορική του υπόσταση.

Θα ήθελα να ευχαριστήσω τους φίλους μου που με συντρόφευσαν σε όλα αυτά τα χρόνια περιπέτειας και μαζί μάθαμε να ονειρευόμαστε χωρίς ταβάνι.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου, που η υπεράνθρωπη υπομονή τους και πίστη στο πρόσωπό μου κάνει αυτά τα όνειρα πραγματικότητα.

## Περίληψη

Η μεταβλητότητα της τιμής του Bitcoin και άλλων κρυπτονομισμάτων είναι ένα από τα μεγαλύτερα εμπόδια που αντιμετωπίζουν τα κρυπτονομίσματα στην εποχή μας. Σε αντίθεση με τα παραστατικά χρήματα, τα σημερινά κρυπτονομίσματα δεν έχουν μια κεντρική τράπεζα που να εφαρμόζει κάποιου είδους νομισματική πολιτική με σκοπό τη διατήρηση της αγοραστικής δύναμης. Αυτό συνεπάγεται ότι μεταβολές στη ζήτηση προκαλούν τεράστιες διακυμάνσεις στη τιμή. Αν οι χρήστες δεν αισθάνονται εντελώς σίγουροι για το ότι η αγοραστική δύναμη του τραπεζικού τους λογαριασμού θα παραμείνει σταθερή από τη μια μέρα στην άλλη, τότε δεν θα υιοθετήσουν ποτέ ένα κρυπτονόμισμα ως το κύριο συναλλακτικό μέσο έναντι ενός σταθερού νομίσματος. Επιπρόσθετα, λόγω της απουσίας σταθερότητας των τιμών, είναι πολύ δύσκολο να χτιστεί μια χρεωστική και πιστωτική αγορά που να βασίζεται στα κρυπτονομίσματα, καθώς κάθε συμφωνία η οποία εμπεριέχει μελλοντικές πληρωμές πρέπει να λαμβάνει υπόψιν και το ρίσκο της μεταβλητότητας της τιμής και να χρεώνει ένα μεγάλο ασφάλιστρο έναντί της.

Παρά το γεγονός ότι υπάρχει πλήθος ερευνών όσον αφορά στα τεχνικά προβλήματα των κρυπτονομισμάτων, όπως η διεκπεραιωτή ικανότητα των συναλλαγών (*transaction throughput*) ή τα *smart contracts*, δεν έχει δοθεί σχεδόν καθόλου προσοχή στο θέμα της βελτίωσης της σταθερότητας των τιμών, πρόβλημα το οποίο είναι πολύ μεγαλύτερο εμπόδιο στη μαζική υιοθέτηση των κρυπτονομισμάτων ως κύριο συναλλακτικό μέσο. Στην παρούσα εργασία, θα παρουσιαστεί το *Dollar Market Token (DMT)*, ένα κρυπτονόμισμα του οποίου τα νομίσματα (*tokens*), μπορούν να διατηρούν αξιόπιστα μια σταθερή ισοτιμία με οποιοδήποτε άλλο αγαθό και ταυτόχρονα να παραμένουν πλήρως αποκεντρωμένα. Συγκεκριμένα, θα επιχειρηθεί να οριστεί ότι 1 DMT μπορεί να εκφραστεί και να ανταλλαχθεί πάντα ως 1 USD. Θεωρητικά, το DMT θα μπορούσε ακόμα και να ανεξαρτητοποιηθεί από το δολάριο και η ισοτιμία του να ορίζεται βάσει ενός αγοραστικού δείκτη τιμής ή κάποιου καλαθιού αγαθών, με τον ίδιο τρόπο που οι κεντρικές τράπεζες υπολογίζουν τον πληθωρισμό και τις πολιτικές που θα ακολουθήσουν. Το DMT επιτυγχάνει τη σταθερότητά του ρυθμίζοντας αλγοριθμικά την προμήθεια των νομισμάτων του βάσει αλλαγών σε μεταβολές του DMT/USD δείκτη. Με αυτό τον τρόπο υλοποιεί ένα είδος νομισματικής πολιτικής παρόμοιο με αυτό που εφαρμόζουν οι κεντρικές τράπεζες σε όλο τον κόσμο. Ταυτόχρονα, λειτουργεί ως ένας αποκεντρωμένος αλγόριθμος, πλήρως διαφανής, βασισμένος σε ένα πρωτόκολλο, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Έτσι, θα μπορούσε να θεωρηθεί το πρωτόκολλο DMT και ως μια αλγοριθμική αποκεντρωμένη κεντρική τράπεζα.

**Λέξεις-κλειδιά:** κρυπτονόμισμα, bitcoin, τεχνολογία blockchain, πρωτόκολλο Dollar Market Token, Seigniorage Shares, MakerDAO, Tether, USDC και BUSD, Bitshares και Ampleforth, AMMs, NFTs

# Algorithmic Stable Coin Without Collateral Assets

## Abstract

Bitcoin and other cryptocurrencies' price volatility is one of the largest entry barriers that cryptocurrencies face today. In contrast to fiat money, cryptocurrencies, do not have a central bank which could implement some monetary policy to maintain their buying power. This in turn is reflected as huge volatility in the price of cryptocurrencies. If users are not confident that the buying power of their money is going to stay relatively the same from one day to the next, they will never adopt a cryptocurrency as their main medium of exchange and they would prefer a stable alternative. Furthermore, given this price volatility, it is very difficult for a credit and debt system to be built on cryptocurrencies, since every agreement which includes future payments must consider the risk that arises from the price volatility and charge a large premium against it.

Although there is a large amount of research related to the technical issues of cryptocurrencies like transaction throughput, smart contract security and optimization concerns, there is very little research regarding the price stability of cryptocurrencies which is the largest barrier for mass adoption. In this dissertation we present the Dollar Market Token protocol (DMT), a cryptocurrency whose tokens can reliably maintain a stable exchange rate with any other asset, and at the same time operate in a fully decentralized manner. Specifically, we attempt to define 1 DMT as being equivalent to 1 USD and keep this exchange rate stable albeit the change in demand. In theory, DMT could even be independent from the dollar and its exchange rate to be based on a consumer-based index or a basket of goods in the same way that the central banks calculate inflation in order to decide on what policy to follow. DMT accomplishes its price stability by adjusting its total circulating supply based on its algorithm specifications. This way it implements some form of monetary policy similar to those implemented by the central banks around the world. At the same time, it operates as a decentralized algorithm which is fully transparent and based only on its protocol specification, independent of any external human intervention. Because of this, DMT can also be perceived as a decentralized central bank.

**Key-words:** cryptocurrency, bitcoin, blockchain technology, Dollar Market Token protocol, Seigniorage Shares, MakerDAO, Tether, USDC and BUSD, Bitshares and Ampleforth, AMMs, NFTs

## Πίνακας Περιεχομένων

Ευχαριστίες .....	6
Περίληψη .....	6
1. Εισαγωγή .....	7
1.1. Κίνητρο .....	7
1.2. Περιγραφή του προβλήματος .....	7
1.3. Στόχοι της διπλωματικής εργασίας .....	9
2. Υπόβαθρο.....	10
2.1. Σχετική Βιβλιογραφία.....	15
2.1.1. Seigniorage Shares.....	15
2.1.2. MakerDAO .....	16
2.1.3. Tether (USDT).....	19
2.1.4. USDC και BUSD .....	19
2.1.5. Bitshares.....	20
2.1.6. Ampleforth.....	21
2.2. Περιπτώσεις χρήσης ενός σταθερού κρυπτονομίσματος.....	22
2.2.1. Αναπτυσσόμενες Αγορές .....	22
2.2.2. Ένα σταθερό νόμισμα για τους επενδυτές.....	23
2.2.3. Χρηματοοικονομικές συμβάσεις .....	24
2.2.4. Η Ευρεία Blockchain Οικονομία .....	25
2.2.5. Καταπολέμηση της Μακροοικονομικής Κρίσης .....	26
3. Μεθοδολογία.....	27
3.1. Το πρωτόκολλο του Dollar Market Token .....	27
3.2. Η Ποσοτική Θεωρία του Χρήματος .....	27
3.3. Τα βασικά μέρη του πρωτοκόλλου Dollar Market Token .....	29
3.4. USD και DMT .....	30
3.5. DebtNFT .....	30
3.6. Automated Market Makers (AMMs) .....	31
3.7. Το Dollar Market Token AMM .....	36
3.8. Πώς το πρωτόκολλο του DMT επιτυγχάνει σταθερότητα στην ισοτιμία.....	37
3.9. Βελτιώσεις .....	39
3.9.1. Ημερομηνία λήξης των ομολόγων.....	39
3.9.2. Πώληση ομολόγων μέσω ανοιχτών δημοπρασιών .....	40
4. Πειράματα & Αποτελέσματα.....	42
4.1. Μεθοδολογία.....	42

4.2. Αποτελέσματα.....	43
5. Συμπεράσματα & μελλοντική εργασία.....	52
5.1. Σταθεροποίηση στο Δείκτη Τιμών του Καταναλωτή .....	52
5.2. Ένα τοπικό Stable νόμισμα για κάθε χώρα.....	53
Βιβλιογραφία .....	54

## Λίστα Πινάκων

Figure 1 Η δομή του blockchain .....	7
Figure 2 Διακλάδωση όταν δύο χρήστες βρίσκουν ταυτόχρονα τη λύση .....	8
Figure 3 Εξίσωση του Stableswap AMM .....	25
Figure 4 Μεταβολή της ποσότητας των δύο αγαθών σε διαφορετικά AMM .....	25
Figure 5 Το φαινόμενο της προσωρινής απώλειας σε σχέση με την αύξηση της τιμής .....	26
Figure 6 Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από USD σε DMT .....	34
Figure 7 Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από USD σε DMT .....	34
Figure 8 Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από DMT σε USD με θησαυροφυλάκιο .....	35
Figure 9 Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από DMT σε USD με θησαυροφυλάκιο .....	35
Figure 10 Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από DMT σε USD χωρίς θησαυροφυλάκιο .....	36
Figure 11 Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από DMT σε USD χωρίς θησαυροφυλάκιο .....	36
Figure 12 Μεταβολή της ισοτιμίας καθώς αγοράζονται Debt NFT .....	37
Figure 13 Μεταβολή της ποσότητας των νομισμάτων καθώς αγοράζονται Debt NFT .....	37
Figure 14 Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από USD σε DMT με εκκρεμή ομόλογα .....	37
Figure 15 Μεταβολή της ποσότητας των νομισμάτων στο AMM από συνεχόμενες ανταλλαγές από USD σε DMT με εκκρεμή ομόλογα .....	37
Figure 16 Μεταβολή της JPY/USD ισοτιμίας στο βάθος τους χρόνου .....	38
Figure 17 Συμπιεσμένο διάγραμμα της μεταβολής της ισοτιμίας JPY/USD στο βάθος του χρόνου .....	39
Figure 18 Απόκλιση του JPY/USD μοντέλου σε σχέση με τα δεδομένα του πραγματικού κόσμου .....	39
Figure 19 Σύγκριση της μεταβολής της ισοτιμίας σε ένα απλό AMM (μπλε) σε σχέση με το DMT AMM (κόκκινο) από συναλλαγές που ακολουθούν το JPY/USD μοντέλο .....	40
Figure 20 Μεταβολές στην ισοτιμία της μετοχής SAVA από το Μάρτιο του 2021 μέχρι το Δεκέμβριο του 2021 .....	41
Figure 21 Απόκλιση του SAVA/USD μοντέλου σε σχέση με τα δεδομένα του πραγματικού κόσμου .....	41
Figure 22 Σύγκριση της μεταβολής της ισοτιμίας σε ένα απλό AMM (μπλε) σε σχέση με το DMT AMM (κόκκινο) από συναλλαγές που ακολουθούν το SAVA/USD μοντέλο .....	42

# 1. Εισαγωγή

## 1.1. Κίνητρο

Η τεχνολογία του blockchain αποτελεί μια από τις σημαντικότερες εφευρέσεις των τελευταίων χρόνων, η οποία προτείνει μια λύση στο μεγάλο πρόβλημα των Βυζαντινών Στρατηγών[1] που αντιμετωπίζουν τα αποκεντρωμένα συστήματα.

Μέσω του blockchain, για πρώτη φορά, οι άνθρωποι μπορούν να ανταλλάσσουν δεδομένα και ταυτόχρονα να διατηρούν μια συμφωνία για την κατάσταση των δεδομένων αυτών χωρίς την ύπαρξη κάποιας κεντρικής βάσης δεδομένων. Αυτό τελευταία, οδήγησε σε ραγδαία ανάπτυξη νέων τεχνολογιών και εφαρμογών που εκτελούνται στο blockchain παρουσιάζοντας διάφορες ομοιότητες με τη γέννηση του διαδικτύου.

Η ύπαρξη ενός κρυπτονομίσματος που εξασφαλίζει μακροπρόθεσμη σταθερότητα της τιμής του είναι ύψιστης σημασίας για την υιοθέτηση των κρυπτονομισμάτων και την χρήση τους σε καθημερινή βάση. Ταυτόχρονα, ένα σταθερό κρυπτονόμισμα θα έλυνε πολλά από τα προβλήματα που αντιμετωπίζουν σήμερα ορισμένες λιγότερο ανεπτυγμένες χώρες με συνέπεια να οδηγούνται συχνά στην υιοθέτηση κάποιου ισχυρότερου ξενικού συναλλάγματος.

Στη διάρκεια των τελευταίων χρόνων έχουν προταθεί διάφορες ακόμη υλοποιήσεις σε σχέση με τα σταθερά κρυπτονομίσματα. Η κάθε μια από αυτές παρουσιάζει επιμέρους πλεονεκτήματα και μειονεκτήματα. Το πιο σημαντικό όμως είναι ότι τα σταθερά κρυπτονομίσματα, για πρώτη φορά προσφέρουν ένα σταθερό νόμισμα, του οποίου η νομισματική πολιτική είναι πλήρως δημόσια και διαφανής για όλους και η οποία καθορίζεται μόνο από τις αντίστοιχες γραμμές κώδικα και όχι από ανθρώπινο φορέα.

Στην παρούσα εργασία, παρουσιάζεται το πρωτόκολλο Dollar Market Token, το οποίο επιτυγχάνει σταθερότητα στην ηθελημένη τιμή του σταθερού νομίσματος στο οποίο προσκολλάται, χωρίς την ανάγκη ύπαρξης φυσικού νομίσματος ως ενέχυρο. Κάτι τέτοιο είναι δυνατό μέσω του αλγορίθμου, ο οποίος συνδυάζει τις λειτουργίες της Κεντρικής Τράπεζας μέσω της μεταβολής της τρέχουσας ποσότητας των νομισμάτων που βρίσκονται σε κυκλοφορία και των μηχανισμών λειτουργίας των αποκεντρωμένων ανταλλακτηρίων. Με αυτό τον τρόπο το πρωτόκολλο DMT προσφέρει μια λύση στο πρόβλημα της σταθερότητας των τιμών ενώ ταυτόχρονα παραμένει πλήρως ανεξάρτητο και διαφανές.

## 1.2. Περιγραφή του προβλήματος

Το γεγονός ότι σήμερα, πολύ λίγοι άνθρωποι στο κόσμο χρησιμοποιούν κρυπτονομίσματα για τις καθημερινές τους συναλλαγές δημιουργεί προβληματισμό.

Θα μπορούσε να ειπωθεί ότι αυτό συμβαίνει επειδή η τεχνολογία των κρυπτονομισμάτων είναι αργή και ακριβή σε σχέση με τα παραδοσιακά μέσα. Παρόλο που κάτι τέτοιο ισχύει ως ένα



βαθμό για το Bitcoin και για πολλά ακόμα κρυπτονομίσματα, δεν ισχύει για μερικά από τα καινούργια πρωτόκολλα. Για παράδειγμα, το κρυπτονομίσμα Solana ισχυρίζεται ότι το δίκτυό του μπορεί να επαληθεύσει νέες συναλλαγές σε λιγότερο από 1 δευτερόλεπτο και ότι μπορεί να υποστηρίξει χιλιάδες συναλλαγές το δευτερόλεπτο, με κόστος λιγότερο από 0.1\$ για κάθε συναλλαγή. Άλλη πιθανή αιτία είναι η ελλιπής αξιοπιστία τους, γεγονός εξίσου αναληθές, καθώς υπάρχει μεγάλος αριθμός από πρωτόκολλα χρηματοδοτούμενα από αξιόπιστες εταιρείες και επενδυτές, αποτελούμενα από πολύ ισχυρές ομάδες προγραμματιστών. Επιπρόσθετα, το ίδιο το Bitcoin έχει αποδείξει ότι το μοντέλο blockchain είναι απίστευτα ισχυρό όσον αφορά στην ανοχή σφαλμάτων ενώ αρκετές φορές αποδείχθηκε πιο ασφαλές από τις παραδοσιακές βάσεις δεδομένων.

Μία άλλη άποψη υποστηρίζει πως τα κρυπτονομίσματα δεν χρησιμοποιούνται ευρέως στην καθημερινότητα λόγω έλλειψης κινήτρου των πωλητών ώστε να αρχίσουν να αποδέχονται κάποιο άλλο είδος πληρωμής πέρα από τις παραδοσιακές, καθώς όλοι οι αγοραστές τους επιλέγουν να/προτιμούν να χρησιμοποιούν το νόμισμα της χώρας. Από την άλλη, με αυτό τον τρόπο χάνουν κάθε πελάτη που θα ήθελε να πληρώσει με κρυπτονομίσματα, ενώ το κόστος εισαγωγής πληρωμών μέσω κρυπτονομισμάτων είναι μηδαμινό. Για την ακρίβεια, επειδή τα κόστη των συναλλαγών μέσω blockchain πολλές φορές είναι πιο μικρά από ότι τα αντίστοιχα για πληρωμές μέσω κάρτας, είναι προς όφελος των πωλητών η επιλογή της πληρωμής μέσω κρυπτονομισμάτων.

Ας παρατηρήσουμε τη θέση ενός πωλητή σήμερα, ο οποίος επιλέγει πληρωμές μέσω κρυπτονομισμάτων [2], όπως για παράδειγμα οι εταιρείες Microsoft ή Spotify, οι οποίες δέχονται πληρωμές με Bitcoin, μέσω της υπηρεσίας BitPay. Φαίνεται ότι οι συγκεκριμένοι πωλητές δεν επιλέγουν να διατηρούν τα κρυπτονομίσματα από τις αγορές τους σε Bitcoin αλλά αντίθετα επιλέγουν να τα μετατρέπουν αυτόματα (ή απευθείας) σε δολάρια. Αυτό συμβαίνει διότι δεν επιθυμούν να έχουν έκθεση στο Bitcoin, ένα νόμισμα το οποίο καθημερινά μπορεί να έχει τεράστιες διακυμάνσεις στην τιμή του. Αν υποθεθεί ότι ξαφνικά η τιμή του Bitcoin μειώνεται κατά 90%, η συγκεκριμένη εταιρεία θα απωλέσει το 90% από τις πωλήσεις της. Επομένως, οι εταιρείες για να επιλέγουν την υιοθέτηση των κρυπτονομισμάτων στα επιχειρησιακά τους μοντέλα, είναι σημαντικό να υπάρχει ένα μέσο αποθηκευτικής αξίας, του οποίου η τιμή να παραμένει σταθερή.

Επίσης, επειδή οι πωλητές για τα αγαθά ή τις υπηρεσίες που παρέχουν επιθυμούν ως αντάλλαγμα κάποιο σταθερό ποσό, σε ευρώ ή δολάρια, θα απαιτούνταν για κάθε συναλλαγή να μεταβάλουν συνεχώς τις τιμές τους σε BTC, με βάση την τιμή του τη δεδομένη χρονική στιγμή. Στον πραγματικό κόσμο, πιθανά προβλήματα από τη χρήση των κρυπτονομισμάτων θα μπορούσαν να συμβούν στην περίπτωση εκείνη που κάποιος πληρώνεται σε BTC και η τιμή του BTC πέφτει ξαφνικά, με συνέπεια να μη διαθέτει αρκετά ώστε να καλύψει τους λογαριασμούς του. Ακόμη, αν κάποιος έχει δανειστεί ένα ποσό από την τράπεζα και οι τόκοι που πληρώνει κάθε μήνα είναι σε BTC, σε περίπτωση που η τιμή του αυξηθεί ραγδαία σε ένα μήνα, είναι πιθανό να μην διαθέτει αρκετά ώστε να αποπληρώσει τους τόκους. Από τα παραπάνω παραδείγματα γίνεται φανερό ότι για να μπορέσουν τα κρυπτονομίσματα να θεωρηθούν ως ένα μέσο ανταλλακτικής αξίας, θα πρέπει να υπάρχει κάποια σταθερότητα στις τιμές.

Κάθε νόμισμα έχει τρεις θεμελιώδεις λειτουργίες: αποθηκευτική αξία, μέσο συναλλαγής και νομισματική μονάδα μέτρησης. Η σταθερότητα στις τιμές είναι ο βασικός πυλώνας για οποιαδήποτε από αυτές τις τρεις λειτουργίες.

Στην παρούσα πτυχιακή παρουσιάζεται το Dollar Market Token, ένα κρυπτονόμισμα το οποίο επιτυγχάνει σταθερότητα στη τιμή του, ενώ ταυτόχρονα παραμένει αποκεντρωμένο, βασισμένο μόνο στον αλγόριθμο που υλοποιεί.

### **1.3. Στόχοι της διπλωματικής εργασίας**

Η παρούσα διπλωματική εργασία έχει ως στόχο την διεκπεραίωση ενός αλγοριθμικού αποκεντρωμένου κρυπτονομίσματος, το οποίο διατηρεί σταθερότητα στην τιμή του χωρίς την ύπαρξη κάποιου ενέχυρου φυσικού αγαθού. Αυτό το σταθερό κρυπτονόμισμα θα πρέπει αφενός να είναι αξιόπιστο κι αφετέρου να διατηρεί σταθερότητα στην τιμή του, ακόμη και σε περιόδους έντονων διακυμάνσεων της ζήτησης. Ταυτόχρονα, ο αλγόριθμός του θα είναι διαφανής και προσβάσιμος από όλους και θα εκτελείται πάνω στο blockchain. Η αποκεντρωμένη φύση του νομίσματος παρέχει μια πληθώρα από πλεονεκτήματα, τα οποία θα παρουσιαστούν σε επόμενες ενότητες.

Στην παρούσα εργασία, το κρυπτονόμισμα θα σταθεροποιηθεί στην τιμή του δολαρίου όπως είναι το σύνηθες και από άλλες υλοποιήσεις σταθερών κρυπτονομισμάτων, αλλά όπως θα υποστηριχθεί στη συνέχεια, θα μπορεί να σταθεροποιηθεί στην τιμή οποιουδήποτε άλλου νομίσματος χωρίς κάποια αλλαγή στον αλγόριθμό του.

## 2. Υπόβαθρο

Το blockchain είναι από τις πλέον δημοφιλείς αλλά και αμφιλεγόμενες εφευρέσεις των τελευταίων χρόνων. Ξεκίνησε όταν ο Satoshi Nakamoto δημοσίευσε το άρθρο “Bitcoin: A Peer-to-Peer Electronic Cash System”[2], όπου περιγράφεται ο τρόπος δημιουργίας ενός ανοιχτού παγκόσμιου δικτύου, το οποίο επιτρέπει την ανταλλαγή νομισμάτων μεταξύ των ενδιαφερόμενων, με έναν τελείως αποκεντρωμένο τρόπο και χωρίς την ανάγκη ύπαρξης κάποιας κεντρικής αρχής. Τα νομίσματα που μπορούν να ανταλλαχθούν σε αυτό το σύστημα τα ονόμασε Bitcoin και η τεχνολογία του δικτύου αργότερα έγινε γνωστό ως blockchain.

Η κατανόηση της λειτουργίας των παραπάνω, προϋποθέτουν την κατανόηση του προβλήματος το οποίο προσπάθησε να λύσει ο Satoshi, μέσα από τη δημοσίευση του άρθρου του. Ένα από τα αρχαιότερα προβλήματα στα πληροφοριακά συστήματα είναι το λεγόμενο πρόβλημα των Βυζαντινών στρατηγών (Byzantine Generals Problem). Το παράδειγμα των Βυζαντινών στρατηγών αφορά ένα φανταστικό πρόβλημα της θεωρίας παιγνίων και των κατακεντρωμένων συστημάτων. Πρόκειται για μια κατάσταση στην οποία κάποιοι στρατηγοί πρέπει να λάβουν μια πολύ κρίσιμη απόφαση σχετικά με το αν θα επιτεθούν ή θα αμυνθούν σε μια συγκεκριμένη στιγμή ενώ ταυτόχρονα κάποιοι από αυτούς δεν είναι αξιόπιστοι. Το πρόβλημα αυτό αποτυπώνει τη δυσκολία της επίτευξης, σε μια τέτοια περίπτωση, μιας γενικής συναίνεσης μεταξύ των στρατηγών αν δεν υπάρχει κάποια κεντρική αρχή και τελικά η παραπάνω κατάσταση παρομοιάζεται με το πρόβλημα εύρεσης μιας ομοφωνίας σε ένα πλήρως αποκεντρωμένο σύστημα, στο οποίο υπάρχουν αναξιόπιστες πηγές. Ο Satoshi, λοιπόν, στην δημοσίευσή του παρουσίασε μια λύση στο παραπάνω πρόβλημα των Βυζαντινών στρατηγών, στην οποία ένα αποκεντρωμένο σύστημα επιτυγχάνει ομοφωνία, παρά την ύπαρξη αφερέγγυων ή κακόβουλων συμμετεχόντων.

Αρχικά, για να λειτουργήσει ένα σύστημα στο οποίο οι συμμετέχοντες μπορούν να ανταλλάσσουν μεταξύ τους χρήματα, θα πρέπει να υπάρχει κάποιος τρόπος ώστε να αποθηκεύεται η κατάσταση του συστήματος αυτού μετά από κάθε συναλλαγή, μέσω ενός λογιστικού βιβλίου. Εδώ ακριβώς έρχεται το πρόβλημα των αποκεντρωμένων συστημάτων, το οποίο έγκειται στο πού θα αποθηκευτεί αυτό το λογιστικό βιβλίο που κρατάει απόδειξη από κάθε συναλλαγή που έγινε στο σύστημα. Αν ο κάθε χρήστης στο δίκτυο κατείχε το δικό του λογιστικό βιβλίο, τότε ενδέχεται να υπάρξουν πιθανές ασυμφωνίες μεταξύ τους. Για παράδειγμα, αν κάποιος χρήστης, έστω η Α, σε αυτό το σύστημα χρωστούσε κάποια χρήματα σε κάποιον άλλο χρήστη, π.χ. τον Β, θα μπορούσε πολύ εύκολα να σημειώσει στο δικό της λογιστικό βιβλίο ότι ξεπλήρωσε τα χρήματα αυτά στον Β και να μην του τα επιστρέψει ποτέ. Όταν στη συνέχεια ερχόταν ο Β για να ζητήσει πίσω τα χρήματα από την Α, αυτή θα αμφισβητούσε ότι του τα χρωστάει ακόμη, καθώς στο δικό της βιβλίο φαίνεται ότι τα έχει ξεπληρώσει. Επειδή το σύστημα είναι πλήρως αποκεντρωμένο, δεν υπάρχει κάποιο κεντρικό λογιστικό βιβλίο το οποίο μπορούν να συμβουλευτούν οι χρήστες για να καταλήξουν σε μια συμφωνία. Αυτό είναι ένα παράδειγμα της δυσκολίας εύρεσης ομοφωνίας σε ένα ανοιχτό αποκεντρωμένο σύστημα. Τα κεντρικά συστήματα δεν αντιμετωπίζουν τέτοιες δυσκολίες καθώς κατέχουν ένα μοναδικό λογιστικό βιβλίο, το οποίο αποθηκεύεται στις διάφορες βάσεις δεδομένων των επιχειρήσεων.

Το σύστημα του Bitcoin παρουσίασε μια λύση στο παραπάνω πρόβλημα όπου κάθε χρήστης κατέχει όπως και προηγουμένως το δικό του λογιστικό βιβλίο. Αυτό έχει τη μορφή αλυσίδας η οποία αποτελείται από blocks, με κάθε block να περιέχει έναν αριθμό από διάφορες συναλλαγές που έγιναν στο σύστημα και μια αναφορά στο προηγούμενο block στην αλυσίδα.

Παρακάτω φαίνεται μια απεικόνιση του λογιστικού βιβλίου και των διαφόρων blocks που αποτελούν το blockchain:

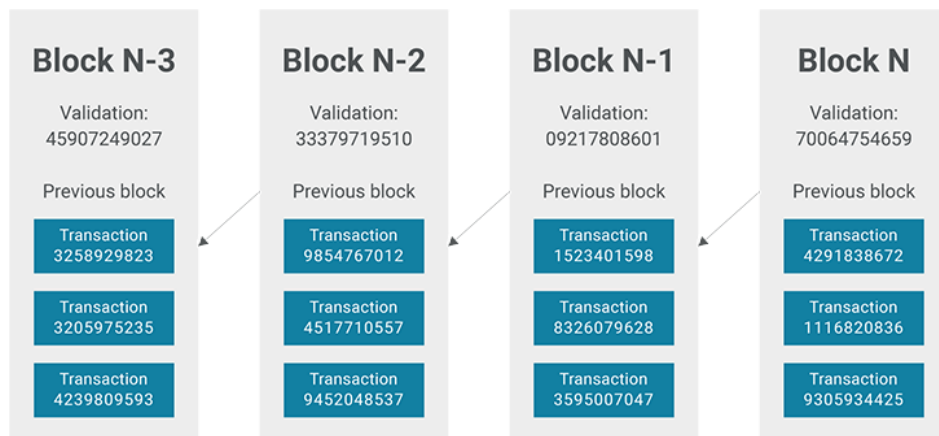


Figure 1. Η δομή του blockchain

Οι συμμετέχοντες παρατηρούν όλες τις συναλλαγές που πραγματοποιούνται στο σύστημα και τις ομαδοποιούν. Έπειτα, μόλις έχουν μαζέψει αρκετές, τις συσκευάζουν σε ένα καινούργιο block και ψάχνουν την λύση σε ένα μαθηματικό πρόβλημα. Η δυσκολία αυτού του μαθηματικού προβλήματος είναι κατά μέσο όρο 10 λεπτά και προσαρμόζεται αναλόγως με το πλήθος των συμμετεχόντων και της υπολογιστικής ισχύος ώστε πάντα ο μέσος όρος επίλυσης του προβλήματος να είναι 10 λεπτά. Μόλις κάποιος χρήστης βρει μια λύση στο συγκεκριμένο πρόβλημα, προσθέτει το καινούργιο block στην τοπική αλυσίδα από blocks που κατέχει και δημοσιεύει αυτό το block μαζί με την απόδειξη επίλυσης του μαθηματικού προβλήματος σε όλους τους υπόλοιπους συμμετέχοντες του δικτύου ώστε να ενημερώσουν και αυτοί το δικό τους λογιστικό βιβλίο. Στην περίπτωση που υπάρχουν παραπάνω από ένα δημοσιευμένα blocks, τα οποία είναι διαφορετικά μεταξύ τους, τότε δημιουργείται μια διακλάδωση (fork) για κάθε ασυμφωνία. Στην περίπτωση αυτή οι συμμετέχοντες περιμένουν για τα επόμενα block και θεωρούν ως έμπιστη την αλυσίδα με τα περισσότερα block.

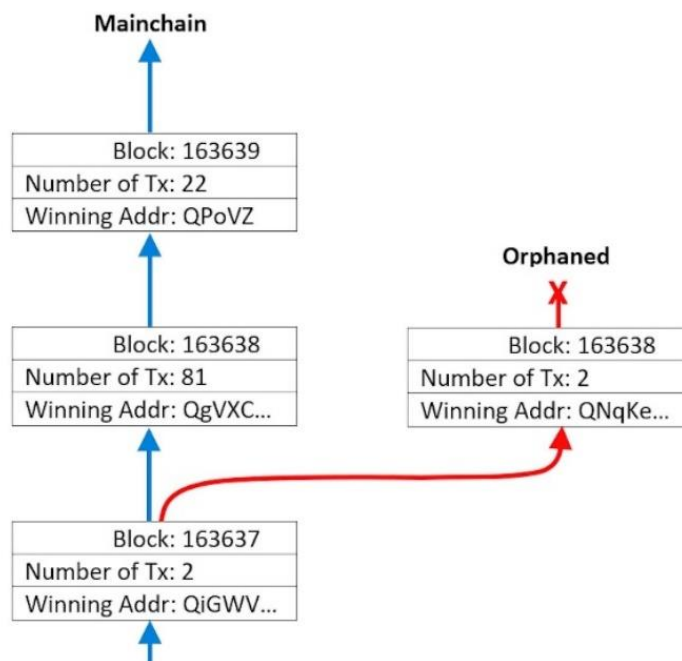


Figure 2. Διακλάδωση όταν δύο χρήστες βρίσκουν ταυτόχρονα τη λύση

Επίσης, ο χρήστης που κατάφερε να βρει πρώτος τη λύση στο μαθηματικό πρόβλημα και δημοσίευσε το καινούργιο block, λαμβάνει ως ανταμοιβή κάποια νέα Bitcoin, που δημιουργεί το πρωτόκολλο καθώς και όλους τους φόρους από τις συναλλαγές του καινούργιου block. Αυτοί οι συμμετέχοντες είναι γνωστοί και ως miners και η επίλυση του μαθηματικού προβλήματος είναι γνωστή ως Proof of Work.

Η ανάγκη ύπαρξης ενός Proof of Work για την ενημέρωση του λογιστικού βιβλίου αποτελεί το κλειδί στην επίλυση του προβλήματος των Βυζαντινών στρατηγών για την επιτυχία μιας κοινής συμφωνίας στα αποκεντρωμένα συστήματα. Το παραπάνω στηρίζεται στη δυσκολία επίλυσης αυτού του προβλήματος, καθώς κάθε ενδιαφερόμενος πρέπει να καταναλώσει υπολογιστικούς πόρους με στόχο να επιλύσει το πρόβλημα πρώτος και να λάβει την ανταμοιβή. Από τη θεωρία παιγνίων προκύπτει ότι δεν συμφέρει κάποιον ενδιαφερόμενο να προσπαθήσει να δημοσιεύσει κάποιο λανθασμένο block επειδή κάποιος από τους άλλους χρήστες θα πάρει την ανταμοιβή και θα έχει καταναλώσει τους υπολογιστικούς του πόρους, χωρίς λόγο. Αν, για παράδειγμα, κάποιος χρήστης κατέχει 30% της συνολικής υπολογιστικής δύναμης του συστήματος, θα έχει πιθανότητα 30% ώστε να βρει την λύση στο επόμενο μαθηματικό πρόβλημα. Στην περίπτωση που καταφέρνει να βρει πρώτος τη λύση, θα πρέπει να καταφέρει να βρει την λύση και στο επόμενο μαθηματικό πρόβλημα, το οποίο έχει πιθανότητα  $0.3 * 0.3 = 0.09$  και να συνεχίσει να το κάνει αυτό ώστε η δική του αλυσίδα, με το λανθασμένο block, να είναι πάντα η μεγαλύτερη και αυτή που ακολουθούν οι χρήστες. Γίνεται φανερό ότι κάτι τέτοιο είναι αδύνατο καθώς οι υπόλοιποι ενδιαφερόμενοι που κατέχουν συνολικά το 70% της υπολογιστικής ισχύος τελικά θα βρίσκουν τα επόμενα blocks με μεγαλύτερη πιθανότητα και θα έχουν την μεγαλύτερη αλυσίδα, με αποτέλεσμα ο κακόβουλος χρήστης να έχει απλά σπαταλήσει υπολογιστική ισχύ. Μια τέτοια επίθεση είναι δυνατή μόνο

στην περίπτωση που κάποιος χρήστης κατέχει 51% ή περισσότερη από τη συνολική υπολογιστική δύναμη, γεγονός που απαιτεί τεράστιο αριθμό κεφαλαίου και πόρων. Επισημαίνεται ότι η δυσκολία του προβλήματος προσαρμόζεται συνεχώς, ανάλογα με την υπολογιστική ισχύ, ώστε να χρειάζεται πάντα 10 λεπτά, κατά μέσο όρο, για την επίλυσή του.

Μέσω του παραπάνω μηχανισμού, το πρωτόκολλο του Bitcoin επιτυγχάνει μια γενική συμφωνία για την τρέχουσα κατάσταση του blockchain, ενώ παραμένει παράλληλα πλήρως αποκεντρωμένη και διαφανής για κάθε χρήστη. Η τεχνολογία του blockchain λοιπόν είναι από τις πιο καινοτόμες εφευρέσεις των τελευταίων χρόνων καθώς επιτρέπει για πρώτη φορά στους χρήστες να ανταλλάσσουν πληροφορία μεταξύ τους, χωρίς την ανάγκη ύπαρξης μιας κεντρικής αρχής, διατηρώντας ταυτόχρονα μια κοινή συμφωνία για την τρέχουσα κατάσταση του συστήματος. Επίσης, αξίζει να σημειωθεί ότι το Proof of Work δεν είναι ο μοναδικός μηχανισμός για την επίτευξη ομοφωνίας στα αποκεντρωμένα συστήματα και ότι έχουν προταθεί διάφορες άλλες εναλλακτικές λύσεις μέσα στα χρόνια [4]. Η πιο γνωστή από αυτές είναι η μέθοδος Proof of Stake, στην οποία οι χρήστες αντί να καταναλώνουν υπολογιστική ισχύ για την επαλήθευση ενός νέου block, παρέχουν κάποια από τα νομίσματα του δικτύου που κατέχουν, ως εγγύηση, ότι λειτουργούν έντιμα. Σε περίπτωση που παρατηρηθεί ότι η συμπεριφορά κάποιου χρήστη είναι κακόβουλη, το σύστημα τον τιμωρεί αφαιρώντας του τα νομίσματα που είχε ως εγγύηση. Κάποια blockchain σήμερα ήδη χρησιμοποιούν αυτή τη μέθοδο έναντι του Proof of Work και το Ethereum σκοπεύει να μεταβεί σε αυτή τη μέθοδο στα μέσα του 2022.

Η τεχνολογία του Bitcoin όμως ήταν μόνο η αρχή στην πορεία των blockchain συστημάτων. Ο Vitalik Buterin παρατηρώντας την δύναμη και τις δυνατότητες του blockchain σκέφτηκε ότι αυτή η τεχνολογία μπορεί να αξιοποιηθεί για την αποθήκευση οποιασδήποτε πληροφορίας και όχι μόνο για την ανταλλαγή χρημάτων. Έτσι το 2013 δημοσίευσε ένα άρθρο στο οποίο περιγράφει τον μηχανισμό ανάπτυξης ενός πλήρως αποκεντρωμένου δικτύου το οποίο θα λειτουργεί ως ένας κεντρικός υπολογιστής και ονόμασε αυτό το δίκτυο Ethereum [5]. Η ιδέα του ήταν ότι κάθε χρήστης σε αυτό το δίκτυο θα μπορεί να δημιουργήσει και να δημοσιεύσει κάποιο πρόγραμμα σε αυτόν τον κεντρικό υπολογιστή, το οποίο μπορεί να εκτελεστεί από τους άλλους χρήστες του συστήματος, αλλάζοντας την κατάσταση του κεντρικού υπολογιστή. Η καθολική κατάσταση του υπολογιστή, όπως και στην περίπτωση του Bitcoin, αποθηκεύεται αποκεντρωμένα στο blockchain και κάθε χρήστης στο δίκτυο συμφωνεί σε αυτή μέσω των ιδίων μηχανισμών ομοφωνίας που περιεγράφηκαν προηγουμένως.

Ο κεντρικός υπολογιστής είναι γνωστός και ως EVM (Ethereum Virtual Machine) και τα προγράμματα που τρέχουν πάνω σε αυτόν είναι γνωστά ως Smart Contracts. Το EVM πρόκειται για ένα αυτόματο στοίβα, του οποίου η τρέχουσα καθολική κατάσταση είναι πλήρως αποκεντρωμένη και κοινή για όλους. Περιέχει ένα σύνολο από εντολές, οι οποίες μεταβάλλουν την τρέχουσα κατάστασή του με ένα ντετερμινιστικό τρόπο. Κάθε συναλλαγή περιέχει μια ή παραπάνω εντολές για το EVM [6] κι έναν φόρο σε ETH, που είναι γνωστός και ως καύσιμο (gas), όπου χρειάζεται για την εκτέλεσή του. Όσο πιο περίπλοκη και χρονοβόρα είναι η συναλλαγή τόσο περισσότερο καύσιμο χρειάζεται να πληρώσει ο αποστολέας για την εκτέλεσή της. Αυτός ο φόρος είναι πολύ σημαντικός καθώς αποτρέπει ατέρμονους βρόχους και πιθανές επιθέσεις DDOS στο σύστημα. Για αυτό το λόγο, το EVM θεωρείται μερικός Turing πλήρης καθώς κάθε βήμα εκτέλεσης είναι περιορισμένο από το αρχικό καύσιμο που

πλήρωσε ο αποστολέας και δεν υπάρχει το πρόβλημα της μη πληρότητας καθώς κάθε πρόγραμμα θα σταματήσει την εκτέλεσή του όταν ξεμείνει από καύσιμα.

Ο Vitalik λοιπόν εμπνευσμένος από την καινοτομία του Bitcoin και τον τρόπο που οι χρήστες μπορούν να ανταλλάξουν χρήματα μεταξύ τους, επέκτεινε τον μηχανισμό αυτό και πρότεινε την δυνατότητα οποιουδήποτε είδους ανταλλαγής δεδομένων με αποκεντρωμένο τρόπο, από ψηφοφορίες μέχρι την ανταλλαγή μηνυμάτων σε μέσα κοινωνικής δικτύωσης ή ακόμη και κάποια κίνηση μέσα σε ένα ηλεκτρονικό βιντεοπαιχνίδι. Με άλλα λόγια, πρόσφερε την δυνατότητα στους χρήστες του δικτύου να δημιουργήσουν και να εκτελέσουν οποιοδήποτε είδος εφαρμογής μπορούν να φανταστούν, διατηρώντας ταυτόχρονα τα δεδομένα στο blockchain, χωρίς την ανάγκη ύπαρξης κάποιου κεντρικού server.

Αυτή η καινοτόμα τεχνολογία του Ethereum ήταν ο καταλύτης και οδήγησε σε μια ραγδαία ανάπτυξη από αποκεντρωμένα προγράμματα και κρυπτονομίσματα, τα οποία τρέχουν πάνω στο δίκτυο του Ethereum, καθώς και την ανάπτυξη νέων blockchain τεχνολογιών που παρομοιάζουν την λειτουργία του Ethereum και κατέχουν το δικό τους οικοσύστημα από προγράμματα. Κάποια από τα πιο δημοφιλή προγράμματα στο Ethereum σήμερα, είναι πρωτόκολλα ανταλλαγής αγαθών, πρωτόκολλα δανεισμού, δυνατότητα επένδυσης σε νέες τεχνολογίες, αποκεντρωμένες οργανώσεις (DAO)[7], ψηφοφορίες και άλλα. Σχεδόν οποιοδήποτε πρόγραμμα μπορεί να σχεδιαστεί με τις παραδοσιακές γλώσσες προγραμματισμού μπορεί επίσης να σχεδιαστεί ώστε να εκτελεστεί αποκεντρωμένα στο δίκτυο του Ethereum, μέσω του κεντρικού υπολογιστή.

Από τα παραπάνω γίνεται αντιληπτό ότι τα κρυπτονομίσματα παρουσίασαν τη λύση στο πρόβλημα των Βυζαντινών στρατηγών, παρέχοντας τα παρακάτω πλεονεκτήματα [8] έναντι των παραδοσιακών κεντρικών συστημάτων[9]:

- **Ασφάλεια:** Όλη η πληροφορία για την τρέχουσα κατάσταση βρίσκεται στα χέρια κάθε χρήστη και όχι μιας κεντρικής βάσης δεδομένων. Έτσι είναι αδύνατο να προκύψει απώλεια αυτής της πληροφορίας λόγω κάποιας βλάβης, καθώς δεν υπάρχει κάποιο μοναδικό σημείο αποτυχίας (Single Point of Failure). [10]
- **Διαφάνεια:** Κάθε συναλλαγή στο blockchain είναι δημόσια και πλήρως διαφανής στον καθένα. Αυτό σημαίνει ότι αν κάποιος ενδιαφερόμενος θελήσει να παρατηρήσει πού μεταφέρονται τα χρήματά του όταν τα αποθηκεύει σε μια αποκεντρωμένη τράπεζα, για παράδειγμα, μπορεί να το κάνει εύκολα παρατηρώντας τις συναλλαγές στο blockchain.
- **Προσβασιμότητα:** Είναι πολύ εύκολο για τον οποιονδήποτε να δημιουργήσει ένα πορτοφόλι και να συμμετάσχει στο blockchain και το μόνο που χρειάζεται είναι πρόσβαση στο διαδίκτυο. Αυτό είναι πολύ σημαντικό καθώς μπορεί να παρέχει πρόσβαση σε χρηματοοικονομικά μέσα, σε ανθρώπους από λιγότερο ανεπτυγμένες χώρες, οι οποίες μπορεί να μην έχουν πρόσβαση σε τράπεζες.

Αν και τα κρυπτονομίσματα παρέχουν λύσεις στα παραπάνω προβλήματα, είναι επίσης γνωστό ότι συνήθως χαρακτηρίζονται από έντονες διακυμάνσεις στις τιμές τους με συνέπεια αυτό να εισάγει ένα μεγάλο εμπόδιο στην πλήρη υιοθέτησή τους στον πραγματικό κόσμο[11].

## 2.1. Σχετική Βιβλιογραφία

Στη διάρκεια των τελευταίων χρόνων, έχουν προταθεί διάφορες υλοποιήσεις σταθερών κρυπτονομισμάτων. Στην παρούσα ενότητα παρουσιάζονται κάποια από αυτά τα πρωτόκολλα και οι τεχνικές που χρησιμοποιούν ώστε να επιτύχουν την σταθερότητα στην τιμή τους.

### 2.1.1. Seigniorage Shares

Το πρωτόκολλο Seigniorage Shares, σε ένα άρθρο που έκδωσε το 2014 [12], εισήγαγε την ιδέα της επιμέρους συστολής και διαστολής της προσφοράς, με σκοπό τη διατήρηση της σταθερότητας του νομίσματός τους. Παρόλο που το πρωτόκολλο του DMT παρουσιάζει ορισμένες ομοιότητες όσον αφορά την λειτουργία του, το Seigniorage Shares εισήγαγε επίσης και κάποιες δυσκολίες στην υλοποίηση του.

Στο πρωτόκολλο Seigniorage Shares, όταν η τιμή των σταθερών νομισμάτων πέφτει, το σύστημα δημιουργεί και προσφέρει ομόλογα νομίσματα σε αντάλλαγμα με τα σταθερά νομίσματα σε μια ανοιχτή δημοπρασία κι έπειτα τα καταστρέφει ώστε να μειώσει την τρέχουσα κυκλοφορία και να επαναφέρει την τιμή. Επίσης, όταν η τιμή του σταθερού νομίσματος αυξάνεται, το πρωτόκολλο δημιουργεί και διανέμει νέα σταθερά νομίσματα σε μια ανοιχτή δημοπρασία, με αντάλλαγμα για ομόλογα, με αποτέλεσμα να μειώνεται η προσφορά των ομολόγων και να αυξάνεται η προσφορά των σταθερών νομισμάτων.

Αυτή η τακτική δημιουργεί τα εξής προβλήματα και δυσκολίες:

- **Δυσκολία στην τιμολόγηση των ομολόγων:** Επειδή το σύστημα προσπαθεί να διατηρήσει την σταθερότητα στις τιμές μέσω της δημοπρασίας σταθερών νομισμάτων σε αντάλλαγμα με ομόλογα κι επίσης ομόλογα σε αντάλλαγμα σταθερών νομισμάτων, είναι πολύ σημαντική η ύπαρξη ενός μηχανισμού τιμολόγησης των ομολόγων. Ενώ το αρχικό άρθρο του πρωτοκόλλου παρουσιάζει έναν θεωρητικό τρόπο τιμολόγησης της τιμής των ομολόγων, υπάρχει η σκέψη ότι στην πράξη έχει κάποια προβλήματα. Το άρθρο ισχυρίζεται ότι αν οι κάτοχοι των ομολόγων συμμετέχουν αναλογικά σε όλες τις δημοπρασίες, τότε μπορούν πάντα να διατηρούν το ίδιο ποσοστό από το συνολικό αριθμό των κυκλοφορούντων ομολόγων. Επειδή, η αθροιστική ανταμοιβή για όλα τα ομόλογα ισούται πάντα με το άθροισμα όλων το μελλοντικών μεταβολών στην προσφορά του σταθερού νομίσματος, αυτό σημαίνει ότι ένα ομόλογο μπορεί να τιμολογηθεί ως το γινόμενο του ποσοστού των νομισμάτων που βρίσκονται σε κυκλοφορία στο παρόν με την συνολική αθροιστική αξία όλων των ανταμοιβών. Αυτό όμως σημαίνει ότι ακόμα κι αν ένας κάτοχος ομολόγων δεν συμμετάσχει σε μια δημοπρασία, το σύστημα θα προσαρμόσει την τιμή των ομολόγων νομισμάτων σαν να είχε συμμετάσχει. Το πρόβλημα με αυτό δημιουργείται όταν υπάρχουν δημοπρασίες οι οποίες έχουν μικρή ρευστότητα. Μια τέτοια δημοπρασία χαμηλής ρευστότητας θα έχει ως αποτέλεσμα την πτώση της τιμής των ομολόγων σε πολύ χαμηλότερα επίπεδα από τα προβλεπόμενα και την δυσaréσκεια των επενδυτών που δεν συμμετείχαν σε αυτή την δημοπρασία. Με άλλα λόγια, οποιαδήποτε δημοπρασία χαμηλής ρευστότητας είναι επιβλαβής για όλους τους επενδυτές οι οποίοι δεν πήραν μέρος σε αυτήν. Κάτι τέτοιο



έρχεται σε αντίθεση με τους μηχανισμούς των περισσότερων οικονομικών συμφωνιών, όπου μια δημοπρασία χαμηλής ρευστότητας είναι επιβλαβής μόνο για τους συμμετέχοντες επενδυτές. Ιδανικά, ο μηχανισμός προσαρμογής του πρωτοκόλλου με βάση την παρούσα ζήτηση θα πρέπει να είναι τελείως ανεξάρτητος από την μελλοντική ρευστότητα. Σε αντίθεση, στο πρωτόκολλο του DMT, οι ανταμοιβές των ομολόγων βασίζονται μόνο στην τρέχουσα Ουρά Ομολόγων και στο μοτίβο των μελλοντικών διακυμάνσεων της τιμής. Ακόμη, είναι πολύ πιο εύκολη η καταπολέμηση προβλημάτων ρευστότητας με τον ορισμό ενός κατώτατου ορίου για την τιμολόγηση των ομολόγων από ότι είναι για τα ομόλογα του Seigniorage Shares καθώς η ανταμοιβή των ομολόγων στην περίπτωση του DMT πρωτοκόλλου είναι πάντα 1 USD.

- **Το πρωτόκολλο δεν μπορεί να επανέλθει από καταστροφικό αποπληθωριστικό κύκλο:** Όταν η ζήτηση των νομισμάτων μειώνεται, το σύστημα του Seigniorage Shares δημιουργεί ολοένα και περισσότερα ομόλογα, με αποτέλεσμα να πέφτουν και άλλοι οι τιμές των ομολόγων. Οι τιμές των ομολόγων μπορούν να επανέλθουν μόνο αν επανέλθει η ζήτηση στο σταθερό νόμισμα, και με άλλα λόγια, το πρωτόκολλο δεν πραγματοποιεί καμία ενέργεια για να παροτρύνει την αύξηση της ζήτησης σε περιόδους πολύ έντονου αποπληθωρισμού και μειωμένης ζήτησης. Αν και το απλό DMT πρωτόκολλο υποφέρει επίσης από αυτό το πρόβλημα, κάτι τέτοιο λύνεται στην περίπτωση που υλοποιηθεί μια ημερομηνία λήξης για τα τρέχοντα ομόλογα, όπως προτάθηκε στις βελτιώσεις. Σε αυτή την περίπτωση, η ζήτηση μπορεί να επανέλθει ακόμη και μετά που οι τιμές των ομολόγων έχουν φτάσει στο 0, καθώς αρκετά από τα ομόλογα θα λήξουν, ανοίγοντας τον δρόμο στην επαναφορά της ζήτησης.
- **Το φαινόμενο των καταστροφικών αποπληθωριστικών κύκλων είναι πολύ πιο σύννηθες:** Όταν η ζήτηση του σταθερού νομίσματος μειώνεται, δεν υπάρχει κάποιο κίνητρο για τους επενδυτές ώστε να αγοράσουν ομόλογα από νωρίς, καθώς όλες οι μετοχές έχουν την ίδια ανταμοιβή, στην ίδια χρονική περίοδο, ανεξάρτητα από το πότε αγοράστηκαν. Αυτό, με τη σειρά του, σημαίνει ότι αν οι άνθρωποι αρχίζουν να υποπτεύονται ότι σύντομα θα υπάρξει πτώση στη ζήτηση των σταθερών νομισμάτων, τότε θα αρχίσουν να πουλούν τα ομόλογά τους και οι τιμές θα πέσουν δραματικά. Είναι επίσης πολύ πιο εύκολο να δημιουργηθεί ένα κλίμα πανικού στο σύστημα του Seigniorage Shares καθώς αν οι τιμές των ομολόγων φτάσουν στο 0, τότε το σύστημα δεν μπορεί να ανταπεξέλθει ξανά, με αποτέλεσμα να υπάρχει ανταγωνισμός για το ποιος θα προλάβει να βγάλει πρώτος τα χρήματά του έξω. Από την άλλη, το DMT πρωτόκολλο, χρησιμοποιώντας μια ουράς προτεραιότητας για την εκπλήρωση των ομολόγων, με βάση την ημερομηνία που δημιουργήθηκαν, ενθαρρύνει τους επενδυτές να αγοράσουν ομόλογα από όσο πιο νωρίς γίνεται. Η ύπαρξη αυτού του επιπλέον κινήτρου μειώνει την πιθανότητα δημιουργίας αποπληθωριστικών κύκλων.

### 2.1.2. MakerDAO

Το πρωτόκολλο του MakerDAO διατηρεί σταθερότητα στην τιμή του νομίσματός του, του λεγόμενου Dai, μέσω μιας τράπεζας αποκεντρωμένων αποθεμάτων. Το πρωτόκολλο του MakerDAO ακολουθεί διαφορετική στρατηγική και επιτυγχάνει σταθερότητα στην τιμή του Dai με την εφαρμογή ενός αποκεντρωμένου συστήματος δανεισμού [13][14].

Πιο συγκεκριμένα, στο MakerDAO, ένας χρήστης μπορεί να βάλει σε υποθήκη κάποιο κρυπτονόμισμα που κατέχει και στη συνέχεια να δανειστεί Dai, με βάση την νομισματική αξία του αγαθού που έβαλε σε υποθήκη. Επειδή οι τιμές των κρυπτονομισμάτων χαρακτηρίζονται από έντονες διακυμάνσεις, η αξία της υποθήκης πρέπει να είναι ίση ή μεγαλύτερη από το 150% της αξίας του δανειζόμενου ποσού. Αυτό σημαίνει ότι αν κάποιος θέλει να δανειστεί για παράδειγμα 400 Dai βάζοντας σε υποθήκη το Bitcoin του, θα πρέπει να κλειδώσει τουλάχιστον 1.5 φορές την αξία του Dai που θέλει να δανειστεί (400 σε αυτό το παράδειγμα), και άρα θα πρέπει να κλειδώσει τουλάχιστον 600\$ Bitcoin.

Χρειάζεται να τονιστεί ότι επειδή η τιμή του Dai είναι σταθερή και ίση με την τιμή του δολαρίου, το ποσό που πρέπει να ξεπληρωθεί είναι πάντα ίσο με το αρχικό ποσό που έχει δανειστεί ο δανειολήπτης, μαζί με έναν επιπλέον τόκο δανεισμού. Κάποιος μπορεί να αναρωτηθεί σε αυτό το σημείο για την αξία μιας τέτοιας ενέργειας, καθώς αν κάποιος κατέχει ήδη 600\$ από Bitcoin γιατί απλά να μην το πουλήσει για να πάρει αυτά τα 400\$ που χρειάζεται; Ο κύριος λόγος είναι ότι αν ένας επενδυτής πιστεύει ότι η αξία του Bitcoin ή του νομίσματος που βάζει ως υποθήκη, θα αυξηθεί στο μέλλον και δεν θέλει να το πουλήσει στη συγκεκριμένη στιγμή, τότε μπορεί να το κρατήσει σε μορφή υποθήκης ενώ ταυτόχρονα μπορεί να χρησιμοποιήσει τα 400\$ που χρειάζεται για κάποια άλλη δραστηριότητα. Επειδή, όπως ήδη αναφέρθηκε, το ποσό που πρέπει να ξεπληρωθεί από το δανεισμό παραμένει σταθερό, αυτό με τη σειρά του σημαίνει ότι αν όντως η τιμή του Bitcoin αυξηθεί στο μέλλον, τότε μπορεί να ξεπληρώσει το δάνειό του και να κρατήσει και την διαφορά από την αύξηση ως κέρδος. Στην αντίθετη περίπτωση, που η αξία της υποθήκης μειωθεί και πέσει κάτω από το 150% της δανειζόμενης αξίας, τότε ο δανειολήπτης θα πρέπει να πληρώσει επιπλέον χρήματα ως ποινή ενώ ταυτόχρονα το πρωτόκολλο μπορεί να ρευστοποιήσει τα χρήματα που έβαλε ως υποθήκη.

Με βάση τα παραπάνω, υπάρχει η δυνατότητα να εξεταστεί ο τρόπος με τον οποίο το MakerDAO επιτυγχάνει σταθερότητα στην τιμή του Dai. Το σύστημα πετυχαίνει σταθερότητα στη τιμή του Dai, προσφέροντας κάποια κίνητρα για δανεισμό ή την επιστροφή των τρεχούμενων δανείων μέσω μεταβολών των επιτοκίων. Αρχικά, όταν κάποιος χρήστης δανείζεται Dai, βάζοντας ένα άλλο αγαθό ως υποθήκη, το σύστημα δημιουργεί και του διανέμει αυτό το Dai, αυξάνοντας έτσι την συνολική προσφορά από Dai, ενώ όταν ξεπληρώνει ένα υπάρχον δάνειο, το πρωτόκολλο καταστρέφει το αρχικό Dai, μειώνοντας την συνολική προσφορά Dai. Το σύστημα του MakerDAO μεταβάλλει λοιπόν τα επιτόκια, με βάση την απόκλιση του Dai από την επιθυμητή τιμή του 1\$. Όσο πιο χαμηλά βρίσκεται η τιμή από το 1\$ τόσο το MakerDAO αυξάνει τα τρέχοντα επιτόκια ώστε να ενθαρρύνει τους χρήστες να ξεπληρώσουν τα δανεισμένα τους Dai. Επειδή το πρωτόκολλο καταστρέφει το Dai που ξεπληρώνουν οι χρήστες, αυτό έχει ως αποτέλεσμα την μείωση της προσφοράς και μακροπρόθεσμα την επαναφορά της τιμής στο 1\$. Αντίθετα, όσο πιο ψηλά βρίσκεται η τιμή από το 1\$, τόσο το MakerDAO μειώνει τα επιτόκια, ενθαρρύνοντας έτσι στους χρήστες να πάρουν νέα δάνεια. Κάθε νέο δάνειο με τη σειρά του δημιουργεί νέα Dai και αυξάνει την συνολική προσφορά και η τιμή πέφτει σταδιακά πίσω στο 1\$. Με αυτό τον τρόπο, η τιμή του Dai παραμένει μακροπρόθεσμα σταθερή στην τιμή του δολαρίου. Τέλος, παρατηρείται ότι και το πρωτόκολλο του MakerDAO εφαρμόζει παρόμοιες ενέργειες με αυτές της Ομοσπονδιακής Τράπεζας Αποθεμάτων, η οποία μεταβάλλει τα επιτόκια για τον έλεγχο του πληθωρισμού ανάλογα με την ζήτηση.

Ακόμη αξίζει να αναφερθεί ότι το πρωτόκολλο του MakerDAO θεωρείται μια πλήρως Αποκεντρωμένη Αυτοματοποιημένη Επιχείρηση (Decentralized Autonomous Organization - DAO). Αυτό σημαίνει ότι αντί να υπάρχει κάποια κεντρική αρχή που ορίζει τις διαφορές παραμέτρους του πρωτοκόλλου και προτείνει μελλοντικές βελτιώσεις, αυτό γίνεται από όλα τα ενδιαφερόμενα μέλη. Για αυτό το λόγο, το MakerDAO πρωτόκολλο προσφέρει ακόμη ένα νόμισμα το MKR, το οποίο λειτουργεί με παρόμοιοι τρόπο με τις μετοχές, δίνοντας την δύναμη στους κατόχους να ψηφίζουν σε μελλοντικές αποφάσεις για το πρωτόκολλο.

Αν και η ιδέα του MakerDAO είναι αρκετά καινοτόμα έχει τα εξής μειονεκτήματα:

- **Δεν υπάρχουν αρκετά κίνητρα για τον δανεισμό Dai:** Αν και το πρωτόκολλο του MakerDAO προσφέρει στους χρήστες την ευκαιρία να δανειστούν χρήματα με έναν αποκεντρωμένο τρόπο, τους παρέχει αυτό το δάνειο πάντα σε Dai. Σε περιόδους όπου η τιμή του Dai καταρρέει, οι ενδιαφερόμενοι δανειολήπτες θα πρέπει είτε να δανειστούν βάζοντας πολύ περισσότερα νομίσματα σε υποθήκη ώστε να είναι ασφαλείς όταν η τιμή του Dai ανέβει ξανά, είτε να πάρουν το ρίσκο να αγοράσουν Dai σε υψηλότερη τιμή, όταν θέλουν να ξεπληρώσουν το δάνειο. Τίποτα από τα δύο δεν είναι ελκυστικό για τους χρήστες, ενώ άλλα ανταλλακτήρια κι άλλες υπηρεσίες δανεισμού προσφέρουν υπηρεσίες με λιγότερο ρίσκο και δυνατότητα δανεισμού περισσότερων κεφαλαίων με την ίδια αξία υποθήκης.
- **Η τιμή του Dai μπορεί εύκολα να φτάσει την τιμή ρευστοποίησης~ 1.5\$:** Αν υποθεθεί ότι η τιμή του ETH καταρρέει, με αποτέλεσμα οι επενδυτές να πουλάνε το ETH τους για σταθερά κρυπτονομίσματα, όπως είναι το Dai, αυξάνοντας την συνολική ζήτηση του. Ταυτόχρονα, πολλοί δανειολήπτες οι οποίοι έχουν βάλει σε υποθήκη το ETH τους και έχουν δανειστεί Dai, θα πρέπει είτε να ξεπληρώσουν τα δάνεια τους ώστε η αξία της υποθήκης τους να μην πέσει κάτω από το 150%, είτε ρευστοποιούνται από το πρωτόκολλο, λόγω της πτώσης της τιμή του ETH που έχουν ως υποθήκη. Επειδή κάθε φορά που ένα δάνειο κλείνει, το δανεισμένο Dai καταστρέφεται, αυτό έχει ως αποτέλεσμα να μειώνεται ταυτόχρονα η προσφορά Dai. Αυτός ο συνδυασμός της αύξησης της ζήτησης με την μείωση της προσφοράς οδηγεί σε μια ραγδαία αύξηση στην τιμή του Dai, με αποτέλεσμα να χάνει την χρησιμότητά του τη στιγμή που οι άνθρωποι το χρειάζονται. Σε μια τέτοια περίπτωση, το πρωτόκολλο βασίζεται στους κατόχους μεγάλων ποσοτήτων από ETH, ώστε να περιορίσουν αυτή την αύξηση παίρνοντας επιπλέον Dai ως δάνειο. Αν εξαιρεθούν αυτοί οι επενδυτές, τότε η τιμή του Dai μπορεί να συνεχίσει να αυξάνεται και να φτάσει την τιμή του 1.5\$, στην οποία περίπτωση οι δανειολήπτες μπορούν να δανειστούν πλέον περισσότερο Dai από την αξία του ETH που βάζουν ως ενέχυρο, δημιουργώντας μια αρμπιτράζ ευκαιρία μηδενικού ρίσκου.

Το MakerDAO καταφέρνει και διατηρεί σταθερή την τιμή του Dai στις μέρες μας, παρά τις δυσκολίες που αναφέρθηκαν. Αυτό το έχει επιτύχει προσφέροντας ελκυστικά κίνητρα στους δανειολήπτες ώστε να χρησιμοποιούν το πρωτόκολλό του, ενώ ταυτόχρονα τα αποθέματα του σήμερα φτάνουν κοντά στην αξία των 10 δισεκατομμυρίων δολαρίων. Παρόλα αυτά, ο χρόνος θα δείξει αν η τιμή του Dai θα παραμείνει σταθερή σε περιόδους πολύ έντονων αναταραχών της αγοράς.

### 2.1.3. Tether (USDT)

Το πρωτόκολλο του Tether [15] και το σταθερό του κρυπτονόμισμα USDT είναι από τα πιο δημοφιλή σταθερά κρυπτονομίσματα, κατέχοντας σήμερα μόλις 78 δισεκατομμύρια συνολικής χρηματιστηριακής αξίας. Το Tether λειτουργεί μέσω μιας επιχείρησης η οποία κρατάει στα αποθέματα της 1 δολάριο για κάθε νέο Tether που δημιουργείται και υπόσχεται στους χρήστες την ανταλλαγή των Tether τους σε δολάρια, όποτε το επιθυμούν. Με άλλα λόγια, το Tether είναι ουσιαστικά μια επιχείρηση, η οποία συσσωρεύει δολάρια και τυπώνει και διανέμει τα δικά της νομίσματα για κάθε δολάριο που κατέχει, παρόμοια με αυτό που έκανε η E-gold στη δεκαετία του '90 με το χρυσό. Η λειτουργία του Tether μπορεί να γίνει με την χρήση μιας κεντρικής βάσης δεδομένων και για αυτό το λόγο το Tether δεν μπορεί να χαρακτηριστεί ακριβώς κρυπτονόμισμα, με τον παραδοσιακό ορισμό των κρυπτονομισμάτων. Αν και η χρήση μιας κεντρικής τράπεζας αποθεμάτων μπορεί να λειτουργήσει βραχυπρόθεσμα, μακροπρόθεσμα παρουσιάζονται αρκετές δυσκολίες.

Κάποιες από αυτές είναι:

- Υπάρχει το ρίσκο να κλείσει η επιχείρηση που διαχειρίζεται αυτά τα αποθέματα δολαρίων, όπως έγινε στην περίπτωση της E-Gold [16]. Επίσης, η ομάδα του Tether είναι αρκετά μυστικοπαθής όσον αφορά τις σχέσεις της με άλλες τράπεζες και παρουσιάζει αρκετά προβλήματα και καθυστερήσεις όταν οι χρήστες θέλουν να εξαργυρώσουν τα Tether τους σε δολάρια. [17][18]
- Επειδή η επιχείρηση του Tether κατέχει το πλήρη έλεγχο των αποθεμάτων, υπάρχει ένα μοναδικό σημείο αποτυχίας.
- Το Tether δεν μπορεί ποτέ να ανεξαρτητοποιηθεί από το δολάριο καθώς, από τη φύση του, όλη του η αξία προέρχεται από τα αποθέματα δολαρίων που έχει στην κατοχή του.
- Δεν υπάρχει κάποια απόδειξη για την ύπαρξη ενός δολαρίου στην τράπεζα αποθεμάτων για κάθε νέο Tether που δημιουργείται. Αυτός είναι ο λόγος που το Tether είχε πρόσφατα κάποια προβλήματα με την Επιτροπή Κεφαλαιαγορών.

Για τους παραπάνω λόγους, το Tether αποτελεί ένα από τα λιγότερο αποκεντρωμένα και πιο επικίνδυνα σταθερά κρυπτονομίσματα σήμερα.

### 2.1.4. USDC και BUSD

Τα USDC [19] και BUSD [20] είναι δυο ακόμα δημοφιλή, σταθερά κρυπτονομίσματα, παρόμοια στη λειτουργία με το USDT, τα οποία διατηρούν την αξία τους σταθερή μέσω μιας τράπεζας αποθεμάτων δολαρίων για κάθε νέο νόμισμα. Σε αντίθεση με το USDT είναι και τα δύο ορθά ρυθμιζόμενα και συμμορφωμένα με την τρέχουσα νομοθεσία καθώς και αρκετά πιο διαφανή, καθώς εκδίδουν πολύ πιο συχνά αναφορές από ελέγχους στην τράπεζα αποθεμάτων τους (η τελευταία αναφορά από την τράπεζα αποθεμάτων του Tether ήταν το 2018). Στην περίπτωση του USDC, η προσφορά του ελέγχεται από ένα δίκτυο από εταιρίες, το Centre Network, και στο οποίο μπορεί να κάνει αίτηση οποιαδήποτε εταιρία, αν τηρεί τις κατάλληλες προϋποθέσεις. Μια από τις εταιρείες του Centre δικτύου είναι και το Coinbase, το οποίο είναι

ένα από τα πιο δημοφιλή ανταλλακτήρια κρυπτονομισμάτων, σήμερα. Στην περίπτωση του BUSD, η προσφορά και η τράπεζα αποθεμάτων ελέγχεται από την εταιρία Paxos.

Αν και τα USDC και BUSD είναι αρκετά πιο διαφανή και ασφαλή στις λειτουργίες τους από το Tether, ωστόσο αντιμετωπίζουν κι αυτά τα ίδια προβλήματα που αναφέρθηκαν στην περίπτωση του USDT.

### 2.1.5. Bitshares

Αξίζει επίσης να σημειωθεί το πρωτόκολλο του Bitshares[21], καθώς ήταν η πρώτη προσπάθεια υλοποίησης ενός σταθερού κρυπτονομίσματος. Το Bitshares μαζί με το σταθερό του κρυπτονόμισμα BitUSD βγήκε στην κυκλοφορία το 2014 στο δικό του Blockchain, το BitShares blockchain και λειτουργεί με τον εξής τρόπο:

- Το πρωτόκολλο αποτελείται από τα BitShares και τα BitUSD νομίσματα.
- Οι επενδυτές μπορούν να ανταλλάξουν μεταξύ αυτών των δυο, σε οποιαδήποτε στιγμή, μέσω μιας υπηρεσίας του BitShare chain.
- Οι επενδυτές μπορούν να στοιχηματίσουν σε δύο πράγματα: είτε στο ότι η τιμή του BitUSD θα αυξηθεί, είτε στο ότι θα μειωθεί.
- Αν θέλουν να στοιχηματίσουν στο ότι η τιμή θα αυξηθεί, τότε απλά αγοράζουν BitUSD από την αγορά και το πουλάνε όταν η τιμή του αυξηθεί για κέρδος. Αυτό έχει ως αποτέλεσμα να αυξάνεται η ζήτηση κι επομένως σταδιακά και η τιμή.
- Όταν θέλουν να στοιχηματίσουν στο ότι η τιμή του BitUSD θα μειωθεί, τότε, δίνουν στο blockchain 1\$ σε BitShares, κλειδώνοντάς το για 30 μέρες. Μετά από τις 30 μέρες υπάρχουν οι εξής περιπτώσεις:
  - **Η τιμή του BitUSD είναι λίγο πιο υψηλή:** Σε αυτή την περίπτωση το πρωτόκολλο τους επιστρέφει λιγότερα BitShares.
  - **Η τιμή του BitUSD είναι αρκετά πιο υψηλή:** Σε αυτή την περίπτωση υπάρχει ο κίνδυνος ρευστοποίησης και ο κίνδυνος να μην τους επιστραφούν καθόλου BitShares.
  - **Η τιμή του BitUSD είναι πιο χαμηλή:** Σε αυτή την περίπτωση τους επιστρέφονται περισσότερα BitShares.
- Όταν κάποιος στοιχηματίζει στο ότι η τιμή του BitUSD θα πέσει κλειδώνοντας το 1\$ του, το πρωτόκολλο στο παρασκήνιο δημιουργεί 1 νέο BitUSD και το πουλάει στην αγορά, αυξάνοντας την συνολική προσφορά από BitUSD. Όπως είναι γνωστό ήδη, η αύξηση της προσφοράς ενώ η ζήτηση παραμένει σταθερή, έχει ως αποτέλεσμα την σταδιακή πτώση της τιμής του BitUSD.
- Τα νέα BitUSD δημιουργούνται μόνο όταν κάποιος έχει αποφασίσει να στοιχηματίσει στο ότι η τιμή θα πέσει χαμηλότερα. Αν κανείς δεν ήταν διατεθειμένος να στοιχηματίσει και να κλειδώσει τα BitShares του, τότε η προσφορά από BitUSD θα παρέμενε σταθερή.
- Με αυτό το τρόπο το BitUSD καταφέρνει να διατηρεί μια σταθερή τιμή μέσω των επενδυτών οι οποίοι στοιχηματίζουν στο ότι η τιμή του νομίσματος θα ανέβει, όταν η τιμή του βρίσκεται κάτω από 1\$, αυξάνοντας έτσι τη ζήτηση και ότι θα πέσει, όταν βρίσκεται πάνω από το 1\$, με αποτέλεσμα να αυξάνουν την συνολική προσφορά του.

Σε γενικές γραμμές το πρωτόκολλο του BitShares έχει αρκετά προβλήματα. Κάποια από αυτά είναι:

- **Ο μόνος λόγος που η τιμή του BitUSD διατηρείται κοντά στη τιμή του δολαρίου είναι επειδή όλοι οι επενδυτές μαζικά πιστεύουν ότι αξίζει 1\$:** Αυτό σημαίνει ότι οι επενδυτές λόγω αυτού του πιστεύω τους είναι αυτοί που κρατούν την ισοτιμία σταθερή, στοιχηματίζοντας συλλογικά ότι θα ανέβει, όταν είναι κάτω από 1\$ και ότι θα πέσει, όταν είναι πάνω από 1\$. Αν ξαφνικά μια μέρα, όλοι οι επενδυτές αποφασίσουν ότι το νόμισμα αξίζει 100\$, τότε η τιμή θα προσαρμοστεί και θα βρει μια νέα ισορροπία στα 100\$. Επίσης, αυτό σημαίνει ότι είναι πολύ κερδοφόρο για έναν επενδυτή να δανειστεί ένα τεράστιο ποσό και να προσαρμόσει μόνος του την τιμή πιο ψηλά. Σε αντίθεση στο πρωτόκολλο του DMT, οι επενδυτές έχουν οικονομικά κίνητρα να διατηρήσουν την τιμή του κοντά στο 1\$.
- **Το BitShares δεν σχεδιάστηκε για αυτό το σκοπό:** Αρχικά το Bitshares δεν δημιουργήθηκε ώστε να υποστηρίζει σταθερά κρυπτονομίσματα, αλλά ώστε να είναι μια αγορά, όπου οι επενδυτές μπορούν να στοιχηματίσουν πάνω σε οποιοδήποτε νόμισμα. Θεωρείται, λοιπόν, ότι η δημιουργία αυτών των σταθερών κρυπτονομισμάτων ήταν απλά μια ευχάριστη σύμπτωση για τους δημιουργούς του Bitshares, χωρίς να έχουν προγραμματίσει κάτι τέτοιο από την αρχή.

### 2.1.6. Ampleforth

Τέλος, είναι ενδιαφέρον να αναφερθεί πώς λειτουργεί το πρωτόκολλο του Ampleforth [22] και το αντίστοιχο νόμισμα AMPL. Αν και το AMPL δεν θεωρείται ακριβώς σταθερό κρυπτονόμισμα, καθώς η τιμή του μεταβάλλεται ανάμεσα σε έναν μέσο όρο και μπορεί να πάρει αυθαίρετο χρόνο ώστε να επιστρέψει στην ισοτιμία του 1\$, υλοποιεί κάποιες αρκετά ενδιαφέρουσες ιδέες, οι οποίες αξίζει να σημειωθούν. Το πρωτόκολλο του Ampleforth προσπαθεί να επιβάλλει σταθερότητα στην τιμή του AMPL, εφαρμόζοντας μια πολιτική γνωστή ως “Rebasing”.

Αυτή η πολιτική είναι αρκετά απλή και λειτουργεί ως εξής:

- Κάθε 24 ώρες το πρωτόκολλο του Ampleforth ελέγχει τη τρέχουσα τιμή του AMPL.
- Αν η τιμή του AMPL είναι περισσότερο από 5% πάνω από τη τιμή του δολαρίου, τότε αυξάνει την ποσότητα των AMPL νομισμάτων που βρίσκονται στο πορτοφόλι των χρηστών.
- Αν η τιμή του AMPL είναι περισσότερο από 5% κάτω από την τιμή του δολαρίου, τότε μειώνει την ποσότητα των AMPL νομισμάτων που βρίσκονται στο πορτοφόλι των χρηστών.
- Αν η τιμή του AMPL βρίσκεται μεταξύ του εύρους του 1\$ +- 0.05, τότε δεν πραγματοποιεί κάποια ενέργεια.
- Το 5% είναι μια δυναμική παράμετρος, παρόμοια με την παράμετρο  $\epsilon$  του πρωτοκόλλου και μπορεί να προσαρμοστεί ώστε να μεταβάλλει το πόσο γρήγορα αντιδρά το πρωτόκολλο σε μεταβολές.

- Οι αυξομειώσεις στην προσφορά γίνονται αυτόματα, χωρίς να χρειάζεται κάποια ενέργεια από τους χρήστες και αναλογικά για όλους τους κατόχους. Αυτό σημαίνει ότι αν κάποιος κατέχει το 1% της συνολικής προσφοράς, πριν το rebase, θα κατέχει το ίδιο ποσοστό από τη συνολική προσφορά και μετά από το rebase.

Από την Ποσοτική Θεωρία του Χρήματος, είναι γνωστό ότι αυτές οι αυξομειώσεις στην ποσότητα των νομισμάτων, που έχουν στην κατοχή τους οι χρήστες, επιτυγχάνουν μακροπρόθεσμη σταθερότητα στην τιμή του AMPL και σύγκλιση στην τιμή του 1\$.

## **2.2. Περιπτώσεις χρήσης ενός σταθερού κρυπτονομίσματος**

Η ανάγκη ύπαρξης ενός αξιόπιστου σταθερού κρυπτονομίσματος σήμερα, είναι μεγαλύτερη από ποτέ. Ένα σταθερό κρυπτονόμισμα θα είχε πολλαπλές χρήσεις, πέρα από τις καθημερινές συναλλαγές, και θα έδινε λύση σε αρκετά προβλήματα που αντιμετωπίζουν τα χρηματοοικονομικά συστήματα. Σε αυτή την ενότητα παρουσιάζονται κάποιες από τις περιπτώσεις χρήσης των σταθερών κρυπτονομισμάτων.

### **2.2.1. Αναπτυσσόμενες Αγορές**

Οι κάτοικοι ανεπτυγμένων χωρών θεωρούν ως δεδομένη την πρόσβαση τους σε σταθερά νομίσματα. Αν για παράδειγμα κάποιος βρίσκεται στις ΗΠΑ, με εύκολη πρόσβαση στο δολάριο, ή στην Ευρώπη, με πρόσβαση στα ευρώ, δεν βρίσκει τον λόγο για την δημιουργία ενός παγκοσμίου, σταθερού κρυπτονομίσματος. Πάραυτα, οι λιγότερο ανεπτυγμένες χώρες, με πιο ασταθή τοπικά νομίσματα, αντιμετωπίζουν προβλήματα υψηλού πληθωρισμού και συνεχόμενης υποτίμησης του νομίσματός τους. Σε αυτές τις χώρες, ένα σταθερό κρυπτονόμισμα θα ήταν εξαιρετικά χρήσιμο.

Για παράδειγμα, τα στατιστικά του 2020 έδειξαν ότι η Αργεντινή υποφέρει από 55% ετήσιο πληθωρισμό και η Τουρκία από 36%. Κι αυτές, είναι μόνο δύο χώρες, οι οποίες έχουν σχετικά σταθερό κυβερνητικό σύστημα. Στη Βενεζουέλα, ο πληθωρισμός τον τελευταίο χρόνο υπολογίστηκε ότι έφτασε περίπου 2000%, το οποίο ουσιαστικά σημαίνει ότι εξαφανίζονται τα χρήματα που κατέχει κάποιος, κάθε χρόνο, κατά 2000%. Αντιμέτωποι με αυτό το πρόβλημα της υποτίμησης του νομίσματος της χώρας τους, οι κάτοικοι αναζητούν άλλες λύσεις για να τα βγάλουν πέρα, και συχνά καταλήγουν στη χρήση του δολαρίου έναντι του τοπικού τους νομίσματος. Αυτό το φαινόμενο είναι γνωστό ως δολαριοποίηση (dollarization). [23] [24]

Συνήθως το φαινόμενο αυτό έχει την παρακάτω εξέλιξη:

- Αρχικά, ένα μέρος του πληθυσμού αρχίζει να υιοθετεί το δολάριο, χωρίς κάποια παρέμβαση από την τοπική κυβέρνηση. Το δολάριο χρησιμοποιείται σήμερα ως το κύριο νόμισμα από πολλές χώρες της κεντρικής Ασίας και της Αφρικής και ο ρυθμός υιοθέτησης αυξάνεται ραγδαία. Για παράδειγμα, σε μόλις δύο χρόνια από το 2006 στο 2008, η δολαριοποίηση στις Σεϋχέλλες αυξήθηκε από 20% στο 60%.

- Έπειτα, η ζήτηση του δολαρίου από τους κατοίκους της χώρας συνεχίζει να αυξάνεται, παρά τις προσπάθειες περιορισμού του φαινομένου αυτού από την κυβέρνηση, μέσω εφαρμογής capital controls και της απαγόρευσης μεταφοράς δολαρίων έξω από την χώρα. Στην Αργεντινή, όταν η κυβέρνηση επέβαλε capital controls το 2011, οι κάτοικοι ίδρυσαν μαύρη αγορά για δολάρια, το λεγόμενο “Dollar blue”[25]. Σε αυτό το διάστημα, υπολογίζεται ότι 10-40 εκατομμύρια δολάρια ανταλλάσσονταν καθημερινά, στη συγκεκριμένη αγορά, με τιμή 25-30% πάνω από την επίσημη ανταλλακτική αξία.
- Τέλος, η υποτίμηση του νομίσματος της χώρας μπορεί να φτάσει σε τέτοιο βαθμό, με συνέπεια η κυβέρνηση επίσημα να υιοθετεί το δολάριο ως το νόμισμα της χώρας, όπως έγινε στην Ζιμπάμπουε το 2009. Σήμερα, ολόκληρη η χώρα χρειάζεται τακτική παραλαβή από κιβώτια δολαρίων.

Γίνεται επομένως εμφανές, ότι εδώ ανοίγεται μια πιθανή ευκαιρία για βελτίωση. Ανεξάρτητα με το αν η δολαριοποίηση είναι επίσημα αναγνωρισμένη, οι κάτοικοι, οι τράπεζες και οι κυβερνήσεις, υφίστανται μεγάλη ζημιά από την φυσική εισαγωγή των δολαρίων. Ένα κρυπτονόμισμα, το οποίο μπορεί να χρησιμοποιηθεί για την μεταφορά εκατομμυρίων δολαρίων, απαιτώντας μόνο ένα κινητό τηλέφωνο ή έναν υπολογιστή συνδεδεμένο στο διαδίκτυο, φαίνεται να είναι μια πολύ πιο ελκυστική λύση από την φυσική μεταφορά χαρτονομισμάτων, στο σενάριο της δολαριοποίησης.

Τέλος, αξίζει να σημειωθεί ότι κάποια υπάρχοντα κρυπτονομίσματα έχουν ήδη αρχίσει να υιοθετούνται από χώρες με υψηλά επίπεδα πληθωρισμού. Σχετικό παράδειγμα αποτελεί και πάλι η Βενεζουέλα, η οποία παρουσιάζει αυξημένη χρήση του Bitcoin στην περίοδο της οικονομικής της κρίσης όπως και το El Salvador, το οποίο πρόσφατα έκανε νόμιμη την χρήση του Bitcoin, για την εκτέλεση οικονομικών συναλλαγών μέσα στη χώρα. Παρόλα αυτά, όπως προαναφέρθηκε, το Bitcoin δεν μπορεί να επιλύσει τα προβλήματα αστάθειας του τοπικού νομίσματος [26] που αντιμετωπίζουν οι κάτοικοι αυτών των χωρών επειδή και το ίδιο είναι ασταθές. Για παράδειγμα, αν το Bitcoin βρίσκεται σε μια φάση υποτίμησης της αξίας του, τότε για τους ανθρώπους που το χρησιμοποιούν δεν έχει κάποια διαφορά από το νόμισμα της χώρας τους [27]. Ένα σταθερό κρυπτονόμισμα επομένως, θα μπορούσε να αποτελεί καταλύτη για χώρες που αντιμετωπίζουν αυξανόμενη υποτίμηση των τοπικών νομισμάτων τους. Σε αντίξοες συνθήκες, αντί να αρχίσουν να εισάγουν χαρτονομίσματα και κέρματα, όπως στην περίπτωση της Ζιμπάμπουε, οι χώρες μπορούν να υιοθετήσουν ένα σταθερό κρυπτονόμισμα.

### **2.2.2. Ένα σταθερό νόμισμα για τους επενδυτές**

Σήμερα, πολλοί επενδυτές κρυπτονομισμάτων τα ανταλλάσσουν σε δολάρια, σε περιόδους μεγάλων αναταραχών της αγοράς. Αυτή η διαδικασία, όμως, παρουσιάζει κάποια προβλήματα.

Αρχικά, κάποια από τα πιο δημοφιλή ανταλλακτήρια στο κόσμο, παρέχουν υπηρεσίες μόνο για κρυπτονομίσματα και όχι για παραστατικά χρήματα. Σε αυτές τις περιπτώσεις, οι επενδυτές έχουν την ανάγκη για ένα σταθερό κρυπτονόμισμα, στο οποίο μπορούν να ανταλλάξουν τα χρήματά τους, μέχρι η αγορά να επανέλθει. Για να καλυφθεί αυτή η ανάγκη, δημιουργήθηκε το USDT-Tether (USDT), όμως για λόγους που θα παρουσιαστούν σε επόμενες ενότητες, μια



λύση όπως αυτή, αντιμετωπίζει αρκετά προβλήματα. Η συνολική αξία της αγοράς του Tether είναι αυτή τη στιγμή γύρω στα 70 δισεκατομμύρια δολάρια, γεγονός το οποίο επιβεβαιώνει την τεράστια ζήτηση για ένα τέτοιο νόμισμα, αλλά επίσης και το ότι δεν μπορεί να ανταπεξέλθει σε αυτήν.

Επιπρόσθετα, τα ανταλλακτήρια τις περισσότερες φορές προσφέρουν τις ανταλλαγές όλων των κρυπτονομισμάτων με ένα βασικό νόμισμα. Προκειμένου οι χρήστες να έχουν τη δυνατότητα να ανταλλάσσουν αποτελεσματικά, θα πρέπει αρχικά να κατέχουν ένα μερίδιο από αυτό το βασικό νόμισμα, κι επίσης να μπορούν εύκολα να αντιλαμβάνονται τις τιμές των κρυπτονομισμάτων σε σχέση με το βασικό νόμισμα. Αν αυτό το βασικό κρυπτονόμισμα ήταν ένα ασταθές κρυπτονόμισμα, όπως είναι το Bitcoin, οι επενδυτές θα χρειαζόταν να μετατρέπουν στο μυαλό τους το Bitcoin που κατέχουν, στο τοπικό νόμισμα της χώρας τους ή στο δολάριο. Οι περισσότεροι επενδυτές, οι οποίοι δεν έχουν πρόσβαση σε αυτοματοποιημένα εργαλεία, θα δυσκολευόντουσαν να κάνουν αυτούς τους υπολογισμούς μόνοι τους, και για αυτό τον λόγο, όλα τα ανταλλακτήρια στον κόσμο που ανταλλάσσουν κρυπτονομίσματα θα επωφελούνταν από ένα κρυπτονόμισμα, όπως το Dollar Market Token.

Μόνο ένα σταθερό κρυπτονόμισμα μπορεί να καλύψει αυτή την ανάγκη των επενδυτών κρυπτονομισμάτων. Επειδή οι επενδυτές κρυπτονομισμάτων είναι από την φύση τους ήδη ανοιχτοί και ενθουσιώδεις για νέα πρωτόκολλα και τεχνολογίες, θα ήταν και οι πρώτοι που θα υιοθετούσαν ένα τέτοιο νόμισμα, όπως είναι το Dollar Market Token.

### **2.2.3. Χρηματοοικονομικές συμβάσεις**

Λόγω της μεταβλητότητάς τους, τα σημερινά κρυπτονομίσματα είναι ακατάλληλα, ακόμη και για τις πιο απλές οικονομικές συμβάσεις στις οποίες στηρίζεται η οικονομία, επειδή αυτές για να λειτουργήσουν, βασίζονται σε κάποια σταθερότητα της τιμής.

Είναι γνωστό ότι το μεγαλύτερο ρίσκο ενός δανειστή, όταν πρόκειται να συνάψει μια σύμβαση για ένα στεγαστικό δάνειο, είναι να μην του επιστραφούν ποτέ τα χρήματα πίσω. Αν αυτό το στεγαστικό δάνειο το διέθετε σε Bitcoin όμως, θα βρισκόταν επίσης εκτεθειμένος στο ρίσκο των μεταβολών της τιμής του Bitcoin. Για παράδειγμα, ένα στεγαστικό δάνειο διάρκειας 30 χρόνων σε Bitcoin, θα έχανε ένα τεράστιο μέρος της αξίας του, αν η τιμή του Bitcoin έπεφτε κατά 90% στα επόμενα 30 χρόνια. Προκειμένου να υπογράψει οποιοδήποτε συμβόλαιο ένας δανειστής, θα χρειαζόταν είτε να έχει τη δυνατότητα να υποθέτει την μελλοντική τιμή του Bitcoin για κάθε δάνειο που επιθυμεί να δώσει, είτε να χρεώνει κάποιον επιπλέον φόρο, λόγω του ρίσκου που έχει από μελλοντικές μεταβολές στην τιμή του Bitcoin. Όπως γίνεται αντιληπτό, αυτό εισάγει παραπάνω δυσκολίες σε μια αρκετά βασική οικονομική συναλλαγή.

Εξ' ορισμού, τα σταθερά νομίσματα δεν αντιμετωπίζουν τέτοιου είδους δυσκολίες, ελαχιστοποιώντας έτσι τα κόστη και αυξάνοντας την ρευστότητα των χρηματοοικονομικών μέσων. Για να διατηρούν την σταθερή τους τιμή, αυτά τα νομίσματα χρειάζονται ακόμη κερδοσκόπους, που είναι διατεθειμένοι να εκτελέσουν τις οικονομικές τους συναλλαγές παρόλες τις αυξομειώσεις στην προσφορά του χρήματος. Ωστόσο, αντί να χρειάζεται να κερδοσκοπούν για κάθε σύμβαση ξεχωριστά, μπορούν πλέον να κερδοσκοπούν μόνο για το ίδιο το νόμισμα, δημιουργώντας έτσι ένα σταθερό, αντισταθμιστικό, ανταλλακτικό

περιουσιακό στοιχείο, το οποίο μπορεί να χρησιμοποιηθεί ως παράγωγο για την συγκρότηση οποιασδήποτε οικονομικής συμφωνίας. Προκειμένου αυτό να γίνει καλύτερα κατανοητό, είναι σαν να παρομοιάζεται ένας κόσμος, στον οποίο κάθε σπίτι χρειάζεται να έχει στην κατοχή του το δικό του μηχάνημα για την παραγωγή ηλεκτρικής ενέργειας, με έναν κόσμο, στον οποίο μια κεντρική μονάδα παραγωγής ηλεκτρικής ενέργειας χρησιμοποιείται για την παραγωγή και την προσφορά της ηλεκτρικής ενέργειας, σε ολόκληρη την πόλη.

Όσο η χρήση των κρυπτονομισμάτων αυξάνεται, είναι αναμενόμενο να αυξάνεται και η ζήτηση για ένα κρυπτονόμισμα, το οποίο να έχει τη δυνατότητα να χρησιμοποιηθεί για τις οικονομικές συμβάσεις[28] του πραγματικού κόσμου, όπως μισθοί, δάνεια, στοιχήματα, συμβόλαια δικαιωμάτων και ούτε κάθε εξής. Προσφέροντας μια σταθερή τιμή, το Dollar Market Token ανοίγει τον δρόμο για την διεξαγωγή αυτών των συμβάσεων [29], με βάση το πρωτόκολλό του.

#### **2.2.4. Η Ευρεία Blockchain Οικονομία**

Αν παρατηρήσει κάποιος τον τομέα του blockchain, θα διαπιστώσει ότι έχει αρχίσει να αναπτύσσεται ένα πλαίσιο από blockchain εφαρμογές, οι οποίες μιμούνται ήδη υπάρχουσες υπηρεσίες, με αποκεντρωμένο τρόπο και εισάγουν συνήθως ένα νόμισμα για τη χρήση του μέσα στην εφαρμογή.

Φυσικά, αν κάθε εφαρμογή στο blockchain δημιουργεί το δικό της νόμισμα, υπάρχει και η ανάγκη για ένα σύστημα συναλλαγής αυτών των νομισμάτων με ένα καθολικό νόμισμα. Ο καθένας επομένως που θέλει να χρησιμοποιήσει αυτή την υπηρεσία, θα χρειάζεται απλά να κατέχει αυτό το καθολικό νόμισμα. Όταν πρόκειται να πληρώσει για την υπηρεσία, αυτό το νόμισμα θα μετατρέπεται, αυτόματα από το σύστημα, στο αντίστοιχο νόμισμα της υπηρεσίας, με βάση την τρέχουσα ανταλλακτική του αξία. Αυτό είναι παρόμοιο με το να διαθέτει κάποιος ένα τραπεζικό λογαριασμό σε δολάρια και να χρησιμοποιεί την πιστωτική του κάρτα σε μια Ευρωπαϊκή χώρα, στην οποία περίπτωση, η τράπεζα αυτόματα χωρίς να το καταλαβαίνει ο ίδιος, μετατρέπει τα δολάρια σε ευρώ στην τρέχουσα ισοτιμία, κάθε φορά που πραγματοποιείται μια συναλλαγή.

Αν το τρέχον πλαίσιο blockchain εφαρμογών εξελιχθεί στο επίπεδο εκείνο, όπου οι blockchain εφαρμογές χρησιμοποιούνται καθημερινά από χιλιάδες χρήστες, για όλες τις υπηρεσίες, είναι αδύνατον αυτό το καθολικό κρυπτονόμισμα να μην έχει μια σταθερή τιμή. Σε ένα αντίθετο σενάριο, θα μπορούσε κάθε πρωί, η τιμή του λεωφορείου που χρησιμοποιεί κάποιος για την μετάβαση στην εργασία του να μεταβάλλεται, σήμερα μπορεί να ήταν 5 ευρώ και αύριο 50. Επιπρόσθετα, ένα κρυπτονόμισμα που παρουσιάζει μεταβλητότητα στην τιμή του είναι ευάλωτο στο πρόβλημα της συσσώρευσης. Αν οι άνθρωποι δηλαδή πιστεύουν ότι η τιμή του νομίσματός τους θα αυξηθεί στο μέλλον, τότε αποφεύγουν να το ανταλλάσσουν και προτιμούν να το συσσωρεύουν. Κάτι τέτοιο θα ήταν καταστροφικό για μια blockchain οικονομία καθώς θα περιόριζε την συνολική ρευστότητα. Από τα παραπάνω γίνεται κατανοητό ότι η ανάπτυξη των blockchain τεχνολογιών και η υιοθέτησή τους συνδέεται στενά με την ύπαρξη ενός σταθερού κρυπτονομίσματος.

### 2.2.5. Καταπολέμηση της Μακροοικονομικής Κρίσης

Ας φανταστούμε έναν κόσμο στον οποίο τα κρυπτονομίσματα έχουν υπερισχύσει έναντι των σημερινών παραστατικών χρημάτων. Όλοι οι άνθρωποι διατηρούν τις οικονομίες τους σε Bitcoin και όλες οι τιμές βασίζονται σε BTC, από τα προϊόντα στο σουπερμάρκετ μέχρι την τιμή ενός νέου σπιτιού ή αυτοκινήτου. Στην περίπτωση αυτή, τίθεται ένα ερώτημα σε σχέση με το τι θα συνέβαινε αν μια υπηρεσία δανεισμού συνάψει αρκετά δάνεια υψηλού κινδύνου με αποτέλεσμα να επαναληφθεί ένα σενάριο παρόμοιο με αυτό της μεγάλης ύφεσης του 2008[30].

Επειδή δεν υφίσταται κάποια ομοσπονδία υπεύθυνη για το Bitcoin, υπάρχει μεγάλο ρίσκο αυτή η ύφεση να εξελιχθεί σε μια μεγάλη μακροοικονομική κρίση. Πολλοί οικονομολόγοι πιστεύουν ότι η ομοσπονδιακή τράπεζα αποθεμάτων με τις δράσεις της απότρεψε την παγκόσμια οικονομία από μια μεγάλη οικονομική κρίση. Αυτό έχει σχέση με το υποθετικό σενάριο που ακολουθεί: βρισκόμαστε σε μια περίοδο οικονομικής ύφεσης, με αποτέλεσμα η ζήτηση για τα αγαθά να μειώνεται. Η πτώση στη ζήτηση συνεπάγεται και πτώση στις τιμές. Όταν όμως οι τιμές εξασθενούν, οι άνθρωποι καταναλώνουν επίσης λιγότερο, αναμένοντας να αγοράσουν σε ακόμη χαμηλότερες τιμές. Προκύπτει για παράδειγμα το ερώτημα, γιατί κάποιος να αγοράσει ένα αμάξι ή να κάνει μια ανακαίνιση στο σπίτι που εκτιμάται σε 10 BTC σήμερα, όταν αυτό μπορεί να κοστίζει μόλις 5 BTC σε ένα χρόνο. Αυτός ο τρόπος σκέψης στη συνέχεια οδηγεί σε ακόμα μεγαλύτερη ύφεση της ζήτησης και ούτω κάθε εξής. Αυτό το φαινόμενο είναι γνωστό και ως “Αποπληθωριστικός κύκλος” (Deflationary Spiral) [31] και αποτελεί την αιτία για εξαιρετικά μεγάλες ζημιές στην παραγωγικότητα της οικονομίας, όπως παρατηρήθηκε και στη μεγάλη κρίση. Ένα εργαλείο που οι κεντρικές τράπεζες χρησιμοποιούν για την καταπολέμηση και την αποφυγή αυτού του αποπληθωριστικού κύκλου, είναι η εφαρμογή μιας επεκτατικής χρηματοοικονομικής πολιτικής, η οποία δημιουργεί και διανέμει νέο χρήμα όσο η τιμές βρίσκονται σε ύφεση. Παρόλα αυτά, ένα τέτοιο είδος δυναμικής νομισματικής πολιτικής είναι αδύνατο να εφαρμοστεί από ένα κρυπτονόμισμα όπως το Bitcoin, καθώς η συνολική προσφορά του είναι σταθερή. Από την άλλη το Dollar Market Token έχει ενσωματωμένη μια δυναμική νομισματική πολιτική στο πρωτόκολλό του και εφαρμόζει κάποιες από τις δράσεις των Κεντρικών Τραπεζών πάνω στο blockchain.

Η τεχνολογία των κρυπτονομισμάτων αναπτύσσεται με ραγδαίους ρυθμούς, σε τέτοιο βαθμό, που σε κάποιο χρόνο, τα κρυπτονομίσματα θα εξυπηρετούν καλύτερα οικονομίες με μεγάλους δείκτες πληθωρισμού, θα είναι πιο βολικά στη χρήση τους από επενδυτές ως ένας σταθερός διαμεσολαβητής από ότι είναι τα μετρητά, και θα δημιουργούν μια βάση πάνω στην οποία να μπορούν να χτιστούν όλες οι διαφορετικές υπηρεσίες της οικονομίας μας. Σέ ένα τέτοιο κόσμο, η ύπαρξη ενός σταθερού κρυπτονομίσματος είναι ύψιστης σημασίας.

### 3. Μεθοδολογία

#### 3.1. Το πρωτόκολλο του Dollar Market Token

Το πρωτόκολλο του Dollar Market Token, για συντομία DMT, επιτυγχάνει τη σταθερότητα στην τιμή του, εφαρμόζοντας παρόμοιες πρακτικές με αυτές των Κεντρικών Τραπεζών σε όλο τον κόσμο[32]. Η πιο σημαντική από αυτές βασίζεται στην Ποσοτική Θεωρία του Χρήματος. Σε αυτή την ενότητα παρουσιάζονται τα επί μέρους θέματα:

- Πώς η Ποσοτική Θεωρία του Χρήματος συνδέει τα μακροπρόθεσμα επίπεδα των τιμών με την προσφορά και την ζήτηση του χρήματος.
- Πώς το πρωτόκολλο DMT υπολογίζει μεταβολές στη ζήτηση, παρακολουθώντας την ισοτιμία του νομίσματος με το αγαθό που αντιπροσωπεύει.
- Πώς το πρωτόκολλο DMT διαστέλλει και συστέλλει την ποσότητα των νομισμάτων που κατέχει με βάση την τρέχουσα ισοτιμία.
- Τα συμφέροντα και οι δράσεις των πιθανών επενδυτών για την διατήρηση της ισοτιμίας του DMT.

#### 3.2. Η Ποσοτική Θεωρία του Χρήματος

Η ιστορία έχει δείξει ότι οι αναταραχές και οι αυξομειώσεις στο χρηματιστήριο και σε άλλες αγορές συνοδεύονται από παρορμητικές ενέργειες των ανθρώπων. Σε περιόδους άνθησης της οικονομίας, οι άνθρωποι έχοντας περισσότερα χρήματα καταναλώνουν περισσότερα αγαθά, με αποτέλεσμα οι τιμές των προϊόντων να αυξάνονται, γεγονός το οποίο με τη σειρά του πυροδοτεί επιπλέον ζήτηση για υψηλότερους μισθούς, με αποτέλεσμα οι άνθρωποι να έχουν ακόμη πιο πολλά χρήματα στη διάθεση τους και ούτω καθεξής. Αυτός είναι ένας πληθωριστικός φαύλος κύκλος που παρατηρήθηκε στην Γερμανία το 1920, στη Βραζιλία το 1980 και στην Αργεντινή το 1990. Παρόμοια, σε περιόδους ύφεσης, οι άνθρωποι φοβούνται να αγοράσουν αγαθά, γεγονός το οποίο συνεπάγεται πτώση της ζήτησης και των τιμών των αγαθών, το οποίο με τη σειρά του ωθεί τους ανθρώπους να περιμένουν να πέσουν επιπλέον οι τιμές για να αγοράσουν αγαθά, με αποτέλεσμα να δημιουργείται ένας ακόμη φαύλος κύκλος. Αυτό το φαινόμενο, όπως αναφέρθηκε στη προηγούμενη ενότητα, είναι γνωστό ως αποπληθωριστικός κύκλος και σχεδόν πραγματοποιήθηκε στην μεγάλη οικονομική κρίση του 2008 [33]. Και στις δυο αυτές περιπτώσεις μια κεντρική τράπεζα μπορεί να παρέμβει για να περιορίσει αυτούς τους καταστροφικούς φαύλους κύκλους. Στη συνέχεια παρουσιάζεται ο τρόπος με τον οποίο θα μπορούσε επιτευχθεί κάτι τέτοιο.

Ας υποθεθεί ότι οι τιμές σε μια οικονομία βρίσκονται σε τέτοιο επίπεδο, στο οποίο το μέσο κόστος για το καλάθι του καταναλωτή αποτιμάται σε 100 ευρώ. Η Ποσοτική Θεωρία του Χρήματος [34] υποστηρίζει ότι αν διπλασιαζόταν τα χρήματα που έχει ο κάθε άνθρωπος στον τραπεζικό του λογαριασμό, αυτό θα είχε ως αποτέλεσμα στο μέλλον το καλάθι του καταναλωτή να κοστίζει 200 ευρώ. Αυτό συμβαίνει επειδή η ονομαστική αξία του χρήματος

έχει διπλασιαστεί, όμως τελικά η αληθινή αξία των αγαθών παρέμεινε ίδια. Αυτό με τη σειρά του σημαίνει ότι οι άνθρωποι είναι διατεθειμένοι να καταναλώσουν ως και τη διπλάσια ονομαστική αξία των χρημάτων τους για να αγοράσουν τα ίδια αγαθά. Το ίδιο συμβαίνει και στην αντίθετη περίπτωση: αν η ονομαστική αξία των χρημάτων που βρίσκονται στο λογαριασμό της τράπεζας του καθενός ξαφνικά μειωνόταν κατά 50%, τότε στο μέλλον το ίδιο καλάθι του καταναλωτή θα κόστιζε μόλις 50 ευρώ.

Εκτείνοντας την παραπάνω θεωρία, μπορεί να παρατηρήσει κανείς την περίπτωση εκείνη κατά την οποία μια κεντρική τράπεζα προσπαθεί να μειώσει τον πληθωρισμό. Οι συνεχόμενες αυξήσεις στις τιμές οδηγούν τους ανθρώπους στο να ξοδεύουν επιπλέον χρήματα. Για να επαναφέρουν τις τιμές οι κεντρικές τράπεζες θα μπορούσαν να μειώσουν τα χρήματα που έχει ο καθένας στην διάθεσή του. Παρόμοια, στην αντίθετη περίπτωση του αποπληθωρισμού, όπου οι άνθρωποι είναι διστακτικοί στην κατανάλωση αγαθών και υπηρεσιών, για να επαναφέρουν τις τιμές οι κεντρικές τράπεζες θα μπορούσαν να προσφέρουν στους ανθρώπους επιπλέον χρήματα. Αν και στην πράξη, τα εργαλεία που χρησιμοποιούν οι κεντρικές τράπεζες για την εφαρμογή αυτών των πολιτικών, είναι συνήθως πιο δυσνόητα και περίπλοκα, όπως για παράδειγμα, πολιτικές ανοιχτής αγοράς και εφαρμογή πολιτικών υποχρεωτικών ελάχιστων αποθεματικών, μια κεντρική τράπεζα από ένα υψηλότερο επίπεδο εφαρμόζει τις εξής δυο λειτουργίες:

- **Διαστολή της προσφοράς χρήματος:** Αν η κεντρική τράπεζα παρατηρεί συνεχή πτώση στις τιμές, μπορεί να αυξήσει την ποσότητα χρήματος που έχει ο κάθε άνθρωπος στην κατοχή του, για να τις επαναφέρει.
- **Συστολή της προσφοράς χρήματος:** Αν η κεντρική τράπεζα παρατηρεί συνεχή αύξηση στις τιμές, μπορεί να μειώσει την ποσότητα χρήματος που έχει ο κάθε άνθρωπος στη διάθεσή του, για τις επαναφέρει.

Η διαστολή και η συστολή της προσφοράς χρήματος λειτουργούν επειδή η Ποσοτική Θεωρία του Χρήματος λέει ότι οι μακροπρόθεσμες τιμές στην οικονομία είναι ανάλογες στην συνολική ποσότητα χρήματος που βρίσκεται σε κυκλοφορία. Ακολουθεί ένα παράδειγμα της θεωρίας για να γίνει καλύτερα αντιληπτό τι θα συνέβαινε αν εφαρμοζόταν από ένα νόμισμα, όπως το DMT, για τη διατήρηση της σταθερότητας της τιμής του:

- Ας υποθεθεί ότι υπάρχει η διάθεση να επιτευχθεί μια σταθερή ισοτιμία μεταξύ του DMT και του δολαρίου, έτσι ώστε 1 DMT νόμισμα να μπορεί πάντα να ανταλλαχθεί με 1 δολάριο. Θαδειχθεί ότι είναι δυνατό να επιτευχθεί αυτό με τη διαστολή ή την συστολή της νομισματικής κυκλοφορίας, ανάλογα με τη διαφορά της τρέχουσας ισοτιμίας από την επιθυμητή.
- Αρχικά, εισάγεται ο ορισμός της αθροιστικής ζήτησης. Η αθροιστική ζήτηση εννοιολογικά δείχνει πόσοι άνθρωποι συνολικά θέλουν το νόμισμα: Ζήτηση = τιμή του νομίσματος \* αριθμός των νομισμάτων που κυκλοφορούν. Αυτή η ποσότητα είναι γνωστή και ως Market cap του νομίσματος.
- Ορίζεται μια μεταβλητή  $X$ , η οποία αναπαριστά το πόσα νομίσματα βρίσκονται σε κυκλοφορία κατά την τρέχουσα χρονική στιγμή, δηλαδή την τρέχουσα προσφορά. Ας υποθεθεί ότι η ζήτηση ανέβηκε τους τελευταίους μήνες και η αξία των νομισμάτων αυτή τη στιγμή είναι 1.10\$. Ζήτηση =  $1.10 * X$ .

- Για να υπολογιστεί πώς μπορεί να προσαρμοστεί η προσφορά ώστε να επανέλθει το νόμισμα στην ισοτιμία του 1\$, ας υποθεθεί ότι η ζήτηση παραμένει σταθερή και ας οριστεί η μεταβλητή  $Y$  ως η επιθυμητή προσφορά:
- Αρχική ζήτηση =  $1.10 * X$
- Τελική ζήτηση =  $1 * Y$
- Αρχική ζήτηση = Τελική ζήτηση
- Λύνοντας για το  $Y$  υπολογίζεται ότι για να επανέλθει η ισοτιμία πίσω στο 1\$ θα πρέπει να αυξηθεί η προσφορά με συντελεστή 1.1:
- $Y = X * 1.1$

Η Ποσοτική Θεωρία του Χρήματος επομένως δείχνει ότι αν το DMT ανταλλάσσεται σε μια τιμή  $P$ , η οποία είναι πιο χαμηλά ή πιο ψηλά από το 1 δολάριο, το πρωτόκολλο μπορεί να επαναφέρει την τιμή πίσω στο 1 δολάριο, πολλαπλασιάζοντας την τρέχουσα προσφορά με τον παράγοντα  $P$ . Υπάρχουν κάποιες ακόμη τεχνικές λεπτομέρειες, οι οποίες θα αναφερθούν σε επόμενες ενότητες, όσον αφορά το πόσο γρήγορα θα πρέπει το πρωτόκολλο να αντιδράσει στις μεταβολές της τιμής, πόσο γρήγορα η τιμή θα επανέλθει πίσω στην επιθυμητή ισοτιμία, αλλά η κεντρική ιδέα της σταθερότητας του νομίσματος βρίσκεται στην συνεχή προσαρμογή της ποσότητας του DMT σε σχέση με αυτή του δολαρίου, ανάλογα με την τρέχουσα ισοτιμία.

### 3.3. Τα βασικά μέρη του πρωτοκόλλου Dollar Market Token

Στην προηγούμενη ενότητα αποδείχτηκε ότι η σταθερή τιμή του DMT επιτυγχάνεται μέσω της προσαρμογής της τρέχουσας προσφοράς από DMT ή USD, ανάλογα με την τιμή. Ακολουθεί ο τρόπος, σύμφωνα με τον οποίο το πρωτόκολλο του DMT υπολογίζει την τρέχουσα τιμή και προσαρμόζει την προσφορά.

Το πρωτόκολλο του DMT αποτελείται από τα εξής μέρη:

- **Automated Market Maker:** Είναι ο πυρήνας του πρωτοκόλλου. Πρόκειται για ένα πλήρως αποκεντρωμένο αλγοριθμικό ανταλλακτήριο, στο οποίο οι χρήστες μπορούν να ανταλλάξουν τα DMT τους για USD και αντιστρόφως. Στην επόμενη ενότητα θα εξηγηθεί με λεπτομέρειες η λειτουργία των Automated Market Makers ή AMM για συντομία.
- **USD:** Πρόκειται για αναπαράσταση του δολαρίου σε μορφή κρυπτονομίσματος. Είναι το νόμισμα με το οποίο υπάρχει η διάθεση να διατηρηθεί μια σταθερή ισοτιμία. Επιλέχθηκε το δολάριο επειδή είναι το πιο ευρεία χρησιμοποιούμενο νόμισμα στον κόσμο των κρυπτονομισμάτων, ωστόσο το πρωτόκολλο μπορεί να λειτουργήσει με οποιοδήποτε άλλο νόμισμα, όπως ευρώ ή ακόμη και BTC ή ETH.
- **DMT:** Το νόμισμα του πρωτοκόλλου που ακολουθεί την τιμή του USD.
- **Θησαυροφυλάκιο (Treasury):** Το πρωτόκολλο σε κάποιες περιστάσεις αποθηκεύει εδώ επιπλέον δολάρια όπως θα εξηγηθεί στη συνέχεια. Με αυτό το τρόπο μειώνει την προσφορά που βρίσκεται στην αγορά ώστε να επαναφέρει την επιθυμητή ισοτιμία.
- **DebtNFT:** όταν η ζήτηση για τα DMT μειώνεται, το πρωτόκολλο εκδίδει κάποια NFT νομίσματα και τα διανέμει σε επενδυτές και ως αντάλλαγμα λαμβάνει USD. Τα

συγκεκριμένα μπορούν να θεωρηθούν και ως τα αντίστοιχα κρατικά ομόλογα που εκδίδει το κράτος και βοηθούν στην επαναφορά της τιμής του νομίσματος, όταν η τιμή του βρίσκεται κάτω από 1\$.

Για να γίνει καλύτερα κατανοητό το πρωτόκολλο του DMT, θα πρέπει πρώτα να αναλυθεί ο τρόπος λειτουργίας κάθε ενός από τα παραπάνω βασικά μέρη.

### **3.4. USD και DMT**

Είναι τα δύο νομίσματα μεταξύ των οποίων είναι επιθυμητή η επίτευξη μιας σταθερής ισοτιμίας. Πρόκειται για κάποια κρυπτονομίσματα που υλοποιούν τα βασικά χαρακτηριστικά των κλασσικών κρυπτονομισμάτων, όπως του ETH. Για την ευκολία και ασφάλεια του κώδικα ακολουθούν τις ERC20 προδιαγραφές της OpenZeppelin [35] βιβλιοθήκης, η οποία είναι μια βιβλιοθήκη που έχει χρησιμοποιηθεί στο βάθος του χρόνου από πολλά ακόμη πρωτόκολλα για την υλοποίηση των κρυπτονομισμάτων τους. Οι ERC20 προδιαγραφές ορίζουν κάποιες βασικές συναρτήσεις που απαιτούνται από όλα τα κρυπτονομίσματα, όπως είναι η δυνατότητα μεταφοράς των νομισμάτων, ο υπολογισμός της ποσότητας που κατέχει ο κάθε χρήστης και λοιπά.

Το USD αποτελεί μια αναπαράσταση του δολαρίου σε μορφή κρυπτονομίσματος και το DMT είναι το νόμισμα που δημιουργήθηκε στο πλαίσιο της παρούσας εργασίας και το οποίο δυνητικά πρέπει πάντα να ανταλλάσσεται για 1 USD. Θα μπορούσε να αντικατασταθεί το USD με οποιοδήποτε άλλο ERC20 κρυπτονόμισμα, όπως για παράδειγμα το ETH και σε αυτή την περίπτωση, το DMT θα ακολουθούσε την τιμή του ETH έναντι του δολαρίου.

### **3.5. DebtNFT**

Όπως θα εξηγηθεί σε επόμενες ενότητες, όταν η τιμή του DMT νομίσματος σε σχέση με το USD πέφτει κάτω από μια ορισμένη αξία, για να επαναφέρει το πρωτόκολλο την τιμή στην επιθυμητή ισοτιμία, εκδίδει και διανέμει κάποια ομόλογα νομίσματα. Αυτά τα ομόλογα νομίσματα είναι σε μορφή NFT. Η διαφορά των NFT έναντι των κλασσικών νομισμάτων είναι ότι, κάθε NFT [36] νόμισμα είναι μοναδικό και αναντικατάστατο από τα υπόλοιπα. Τα κλασσικά νομίσματα, όπως και τα παραστατικά νομίσματα, θεωρούνται ότι έχουν όλα μια κοινή αξία ενώ τα NFT νομίσματα μπορούν να έχουν το καθένα τη δική τους αξία.

Για τους λόγους που αναφέρθηκαν στη προηγούμενη ενότητα, έγινε και πάλι η χρήση της OpenZeppelin βιβλιοθήκης για την υλοποίηση των βασικών λειτουργιών. Οι προδιαγραφές για NFT είναι οι ERC721 [37] και παρέχουν τη βασική λειτουργικότητα που απαιτείται από όλα τα NFT νομίσματα. Επιπλέον, το DebtNFT περιέχει κάποιες πρόσθετες λειτουργίες, ώστε να μπορεί να χρησιμοποιηθεί σαν ομόλογο. Όταν δημιουργείται για πρώτη φορά, μεταφέρεται στο πορτοφόλι του χρήστη που αγόρασε το συγκεκριμένο χρεωστικό ομόλογο και αποθηκεύει το ποσό που οφείλει να του ξεπληρώσει. Έπειτα, στο μέλλον, όταν ικανοποιηθούν κάποιες συνθήκες οι οποίες θα αναλυθούν στις επόμενες ενότητες, το πρωτόκολλο διανέμει τις πληρωμές που οφείλει στους κατόχους αυτών των NFT νομισμάτων.

Ο λόγος που έγινε η χρήση ενός NFT νομίσματος έναντι ενός παραδοσιακού κρυπτονομίσματος, είναι ότι με αυτό τον τρόπο τα ομόλογα νομίσματα μπορούν πολύ εύκολα να ανταλλαχθούν από τους χρήστες, σε υπάρχουσες NFT αγορές. Επειδή κάθε DebtNFT, από την φύση του, είναι ξεχωριστό και περιέχει μέσα του όλη την πληροφορία ώστε να μπορεί ο κάτοχός του να ξεπληρωθεί, οι χρήστες μπορούν εύκολα να το ανταλλάξουν σε μια υπάρχουσα NFT αγορά, όπως είναι το Opensea [38] ή το LooksRare [39], στην τιμή που επιθυμούν. Σε αντίθετη περίπτωση, κατά την οποία το νόμισμα θα ήταν ένα παραδοσιακό κρυπτονόμισμα, για λόγους που θα παρουσιαστούν στην επόμενη ενότητα, θα χρειαζόταν να προσφερθεί ρευστότητα σε ένα από τα υπάρχοντα αποκεντρωμένα ανταλλακτήρια, για κάθε νόμισμα που υπάρχει η επιθυμία να μπορεί να ανταλλαχθεί για DebtNFT.

### 3.6. Automated Market Makers (AMMs)

Προκειμένου να γίνει κατανοητός ο τρόπος με τον οποίο είναι χτισμένο το ανταλλακτήριο του DMT πρωτοκόλλου και το πώς επιτυγχάνει μακροπρόθεσμα μια σταθερή ισοτιμία μεταξύ των USD και DMT νομισμάτων, θα πρέπει αρχικά να κατανοηθεί ο όρος Automated Market Maker ή AMM, χάριν συντομίας.

Τα AMM είναι κάποια πρωτόκολλα [40] που δημιουργήθηκαν τα τελευταία χρόνια και στα οποία μπορούν οι χρήστες να ανταλλάσσουν τα νομίσματά τους πλήρως αποκεντρωμένα, χωρίς την ύπαρξη κάποιας κεντρικής αρχής. Αρχικά, τα παραδοσιακά ανταλλακτήρια επιτρέπουν στους χρήστες να ανταλλάσσουν τα νομίσματά τους μεταξύ τους, με την χρήση ενός κεντρικού βιβλίου παραγγελιών. Κάθε φορά που ένας χρήστης θέλει να ανταλλάξει ένα νόμισμα που κατέχει με κάποιο άλλο, τότε προσδιορίζει την ποσότητα των νομισμάτων που θέλει να αγοράσει και την τιμή. Στη συνέχεια, αυτή η πληροφορία εισάγεται στο κεντρικό βιβλίο παραγγελιών και το σύστημα ψάχνει για καταχωρήσεις άλλων χρηστών, οι οποίοι επιθυμούν να πουλήσουν το συγκεκριμένο νόμισμα, το οποίο θέλει να αγοράσει στη τιμή που προσδιόρισε. Αν βρεθεί μια ή περισσότερες καταχωρήσεις, οι οποίες ικανοποιούν αυτές τις συνθήκες, τότε το σύστημα πραγματοποιεί αυτή την συναλλαγή και τις απαλείφει από το βιβλίο παραγγελιών. Τέλος, η τιμή του νομίσματος αλλάζει στην τιμή της τελευταίας ανταλλαγής που πραγματοποιήθηκε.

Η παραπάνω μέθοδος, αν και χρησιμοποιείται εδώ και αρκετά χρόνια και είναι αρκετά αποτελεσματική, έχει και τα μειονεκτήματά της. Αυτά βασίζονται κυρίως στο ότι το βιβλίο παραγγελιών βρίσκεται σε μια κεντρική βάση δεδομένων του ανταλλακτηρίου και τα διαχειρίζεται μια κεντρική αρχή και είναι τα εξής:

- Ο αλγόριθμος, μέσω του οποίου γίνεται η ανταλλαγή των αγαθών, είναι ιδιωτικός και πρέπει να υπάρχει εμπιστοσύνη μεταξύ των επενδυτών που ανταλλάσσουν και του ανταλλακτηρίου που κατέχει το βιβλίο αγορών. Για παράδειγμα, η εταιρία θα μπορούσε να προσφέρει στους ενδιαφερόμενους πάντα μια χειρότερη ισοτιμία από την πραγματική, κρατώντας κάποια επιπλέον νομίσματα από την συναλλαγή ή σε περιπτώσεις όπου το βιβλίο παραγγελιών είναι γεμάτο, να δίνει προτεραιότητα σε κάποιους χρήστες.
- Η εταιρεία εισάγει έναν φόρο για κάθε ανταλλαγή και συνήθως ένα ελάχιστο ποσό που πρέπει να ανταλλαχθεί και μπορεί να αλλάζει αυτές τις παραμέτρους, όποτε επιθυμεί.



- Αν ο κεντρικός server του ανταλλακτηρίου διακοπεί, τότε οι χρήστες δεν μπορούν να ανταλλάξουν τα νομίσματά τους.
- Αν το βιβλίο παραγγελιών έχει κάποιο πρόβλημα στον κώδικα ή η βάση δεδομένων δεχτεί κάποια επίθεση και μεταβληθούν τα δεδομένα, τότε θα πραγματοποιηθούν λάθος ανταλλαγές.
- Το ανταλλακτήριο αποθηκεύει επίσης τα νομίσματα κάθε χρήστη στην κεντρική βάση δεδομένων του. Σε περίπτωση που αυτό δεχτεί κάποια επίθεση, τότε μπορούν να κλαπούν τα νομίσματα των χρηστών. Ένα από τα πιο γνωστά παραδείγματα μιας τέτοιας επίθεσης, είναι η επίθεση που έγινε στο Mt. Gox, ένα από τα πιο δημοφιλή ανταλλακτήρια για BTC και κλάπηκαν 850 χιλιάδες Bitcoin.

Παρατηρώντας λοιπόν τα παραπάνω προβλήματα των κεντρικών ανταλλακτηρίων και με τη βοήθεια των blockchain αποκεντρωμένων λειτουργιών, οι άνθρωποι σκέφτηκαν και κατασκεύασαν έναν αλγόριθμο, με τον οποίο όλοι οι χρήστες μπορούν να ανταλλάσσουν νομίσματα μεταξύ τους, χωρίς την ανάγκη ύπαρξης κάποιου κεντρικού φορέα ή κάποιας κεντρικής βάσης δεδομένων.

Τα πιο δημοφιλή από αυτά τα πρωτόκολλα, είναι γνωστά ως Automated Market Makers και πρόκειται για πλήρως αποκεντρωμένα προγράμματα, τα οποία τρέχουν στο blockchain και επιτρέπουν στους χρήστες να ανταλλάσσουν μεταξύ τους τα νομίσματά τους, χωρίς να βασίζονται σε ένα κεντρικό βιβλίο παραγγελιών. Αυτά λύνουν όλα τα προβλήματα που αναφέρθηκαν παραπάνω καθώς ο αλγόριθμός τους είναι δημόσιος και πλήρως διαφανής, τρέχουν πάνω στο blockchain, οπότε η λειτουργία τους δεν βασίζεται στην λειτουργία ενός κεντρικού server και τέλος, κάθε χρήστης έχει στην κατοχή του τα νομίσματά του, σε ένα προσωπικό του πορτοφόλι.

Τα AMM λειτουργούν ως εξής:

- Το πρωτόκολλο έχει στην κατοχή του κάποια ρευστότητα από ζευγάρια νομισμάτων, τα οποία μπορούν να ανταλλαχθούν μεταξύ τους. Τα ζευγάρια αυτά είναι γνωστά και ως Liquidity Pools ή LP, για συντομία.
- Οι χρήστες μπορούν να ανταλλάσσουν τα νομίσματα τους, αφήνοντας ένα νόμισμα που κατέχουν και παίρνοντας κάποιο άλλο από το αντίστοιχο LP.
- Αν για παράδειγμα το ανταλλακτήριο έχει ένα ETH/USD LP και ένας χρήστης θέλει να ανταλλάξει το ETH που έχει στην κατοχή του με USD, τότε θα δώσει την ποσότητα από ETH που θέλει να πουλήσει στο LP και θα πάρει μια ποσότητα από USD από αυτό.
- Η τιμή των νομισμάτων υπολογίζεται με βάση την αναλογία των νομισμάτων στη δεξαμενή ρευστότητας και μιας εξίσωσης που μπορεί να ορίσει διαφορετικά το κάθε AMM πρωτόκολλο. Με βάση αυτή την εξίσωση υπολογίζεται επίσης το πόσα νομίσματα θα πάρει ο χρήστης σε αντάλλαγμα για τα νομίσματα που άφησε στο LP.
- Στο παράδειγμα όπου ο χρήστης κατέθεσε ETH, αυξάνοντας την ποσότητα των ETH και μειώνοντας την ποσότητα των USD στο LP, ο χρήστης μετέβαλε την τρέχουσα αναλογία τους και επομένως και την τιμή.
- Σε γενικές γραμμές, όταν η αναλογία είναι 1:1, δηλαδή υπάρχει ακριβώς η ίδια ποσότητα στο LP από τα δύο, σημαίνει ότι τα νομίσματα έχουν ακριβώς την ίδια αξία. Όταν επίσης αυξάνεται η ποσότητα του ενός νομίσματος x και μειώνεται η ποσότητα

του άλλου  $y$ , σημαίνει ότι η τιμή του  $x$  σε σχέση με το  $y$  μειώνεται και αντίστροφα. Στο παράδειγμα, επειδή αυξήθηκε η ποσότητα από ETH και μειώθηκε η ποσότητα από USD στο LP, αυτό οδήγησε στην πτώση της τιμής του ETH ως προς το USD, με βάση την εξίσωση που ορίζει ο αλγόριθμος.

Η πιο συνηθισμένη εξίσωση που χρησιμοποιείται από τα AMM's είναι η  $x * y = k$ , όπου  $x$  και  $y$  είναι η ποσότητα από το κάθε νόμισμα στο LP και  $k$  είναι μια σταθερά, η οποία αντιπροσωπεύει την συνολική ρευστότητα της δεξαμενής ρευστότητας. Η σταθερά  $k$  μας λέει ότι η συνολική ρευστότητα του LP πριν και μετά την ανταλλαγή πρέπει να παραμείνει σταθερή και με βάση αυτή, υπολογίζεται το ποσό των νομισμάτων που πρέπει να αφήσει ένας χρήστης στο LP, όταν θέλει να ανταλλάξει ένα νόμισμα. Ακολουθεί παράδειγμα για να γίνει καλύτερα κατανοητή η λειτουργία αυτού:

- Ας θεωρηθεί ότι υπάρχει ένα LP μεταξύ του ETH/USD στο AMM, ώστε να μπορούν οι χρήστες να ανταλλάσσουν ETH με USD και αντιστρόφως.
- Επίσης, ας υποτεθεί ότι η δεξαμενή ρευστότητας στην παρούσα χρονική στιγμή έχει 10 ETH και 150 USD, άρα  $x_{\text{αρχικό}} = 10$  και  $y_{\text{αρχικό}} = 150$  και λόγω της εξίσωσης  $x * y = k$ , το  $k$  ισούται με 1500.
- Η τιμή του  $x$  ως προς το  $y$  μπορεί να υπολογιστεί διαιρώντας την ποσότητα  $y$  με το  $x$ . Στο παράδειγμα λοιπόν η του 1 ETH είναι ίση με 15 USD.
- Αν ένας χρήστης τώρα θέλει να πουλήσει 5 ETH, αυτό σημαίνει ότι θα αυξήσει την ποσότητα  $x$  στο LP κατά 5, και άρα  $x_{\text{τελικό}} = 15$ .
- Υπολογίζεται τώρα η τελική ποσότητα  $y$  στην δεξαμενή ρευστότητας από την εξίσωση  $x_{\text{τελικό}} * y_{\text{τελικό}} = k$ , η οποία πρέπει πάντα να διατηρείται. Λύνοντας ως προς  $y_{\text{τελικό}}$  υπολογίζεται η ποσότητα από  $y$  στο LP μετά την ανταλλαγή να είναι:  $y_{\text{τελικό}} = k / x_{\text{τελικό}}$ . Το  $k$  είναι σταθερό και ίσο με 1500 και το  $x_{\text{τελικό}}$  υπολογίστηκε ως 15, και άρα υπολογίζεται ότι το  $y_{\text{τελικό}}$  θα πρέπει να είναι ίσο με  $1500 / 15 = 100$ .
- Αν τώρα αφαιρεθεί το  $y_{\text{τελικό}}$  από το  $y_{\text{αρχικό}}$  υπολογίζεται η ποσότητα από USD που θα πάρει σε αντάλλαγμα ο χρήστης για τα 15 ETH που άφησε, το οποίο είναι στο παράδειγμα  $150 - 100 = 50$ . Άρα για τα 15 ETH που άφησε θα πάρει σε αντάλλαγμα 50 USD.
- Επειδή η τιμή του  $x$  ως προς το  $y$  υπολογίζεται από τη σχέση Τιμή =  $y / x$  μπορεί να υπολογιστεί η νέα τιμή ως:  $\text{ETH}_{\text{τελικό}} = y_{\text{τελικό}} / x_{\text{τελικό}} = 100 / 15 = 6.66$  USD. Όπως φαίνεται, μεταβάλλοντας τις ποσότητες  $x$  και  $y$  στο LP, η τιμή του ETH ως προς το USD έπεσε από τα 15 στα 6.66 USD, το οποίο είναι το αναμενόμενο, καθώς ο χρήστης πούλησε ETH για USD.
- Μπορεί επίσης να υπολογιστεί το ποσοστό της μεταβολής της τιμής του ETH από αυτή την συναλλαγή από την εξίσωση:  $(\text{τελική τιμή} - \text{αρχική τιμή}) / \text{αρχική τιμή}$ . Στην συγκεκριμένη περίπτωση είναι:  $(6.66 - 15) / 15 = -0.556$  ή -55.6%, δηλαδή η τιμή του ETH σε σχέση με το USD μειώθηκε κατά 55.6% από αυτή την συναλλαγή. Αυτό είναι γνωστό και ως slippage ή price impact. Το slippage εξαρτάται από δύο παράγοντες, το ποσό της συναλλαγής και το  $k$ . Καταρχήν, όσο πιο μεγάλο είναι το μέγεθος της συναλλαγής, τόσο μεγαλύτερο είναι και το slippage. Δηλαδή αν είναι επιθυμητή η ανταλλαγή αντί για 5 ETH, 5 χιλιάδες ETH, το slippage θα αυξανόταν. Επίσης, όσο πιο μεγάλο είναι το  $k$ , δηλαδή η συνολική ρευστότητα, τόσο πιο μικρό είναι το slippage. Για παράδειγμα, αν υπήρχε αρχική ρευστότητα  $k = 1,5$  δισεκατομμύρια στο LP αντί για 1500, τότε το slippage, από την ίδια ενέργεια, θα ήταν μόλις -0.13%.

Η εξίσωση  $x * y = k$  χρησιμοποιείται από πρωτόκολλα, όπως το Uniswap, Sushiswap, Pancakeswap και αν και είναι η πιο δημοφιλής, δεν είναι η μοναδική. Κάποια άλλα πρωτόκολλα χρησιμοποιούν την εξίσωση  $x + y = k$  ή και πιο σύνθετες, όπως αυτή του StableSwap [41]:

$$An^n(x_j + \sum_{i \neq j} x_i) + D = ADn^n + \frac{n^{n+1}}{n^n x_j \prod_{i \neq j} x_i}$$

Figure 3. Εξίσωση του Stableswap AMM

Στο παρακάτω διάγραμμα απεικονίζεται η μεταβολή της ποσότητας  $y$  σε σχέση με μεταβολές στην ποσότητα  $x$ , γι αυτές τις τρεις διαφορετικές εξισώσεις:

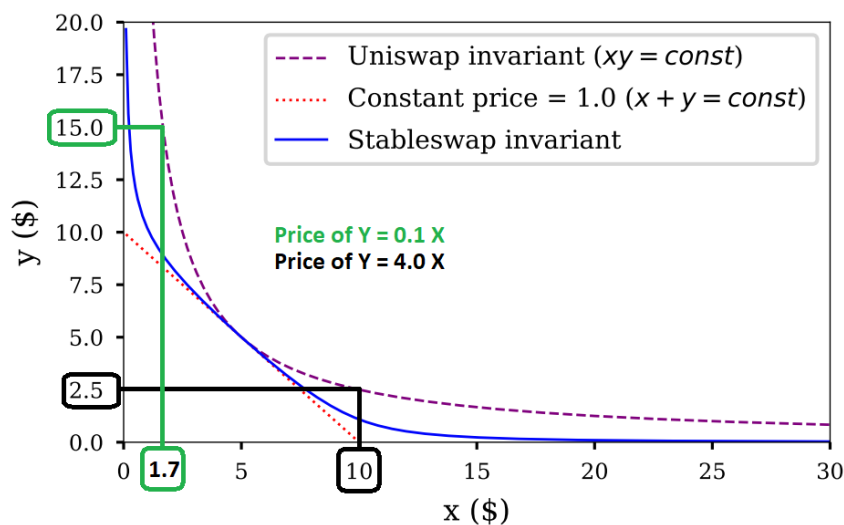


Figure 4. Μεταβολή της ποσότητας των δύο αγαθών σε διαφορετικά AMM

Όπως φαίνεται, κάθε μια από αυτές τις εξισώσεις μεταβάλλει την ποσότητα  $y$  κι επομένως την τιμή, διαφορετικά για την ίδια μεταβολή  $x$ . Επίσης παρατηρείται ότι όσο το  $x$  τείνει στο 0 ή στο άπειρο, τόσο μεγαλύτερες είναι οι μεταβολές στο  $y$  και δηλαδή, ότι ο χρήστης πρέπει να πληρώσει εκθετικά μεγαλύτερη ποσότητα από  $x$  για την ίδια ποσότητα  $y$ .

Εξηγήθηκε λοιπόν η λειτουργία των AMM's και πώς υπολογίζουν την τιμή ενός νομίσματος σε σχέση με ένα άλλο, με βάση την εξίσωσή τους και την τρέχουσα αναλογία των νομισμάτων στο LP. Κάποιος όμως μπορεί να αναρωτιέται από πού προέρχεται η συνολική ρευστότητα των νομισμάτων για κάθε LP. Η απάντηση είναι ότι οποιοσδήποτε χρήστης μπορεί να παρέχει ρευστότητα σε ένα LP, αυξάνοντας την συνολική ρευστότητα και βοηθώντας στην ανταλλαγή αυτών των νομισμάτων. Για να το κάνει αυτό πρέπει να έχει στη κατοχή του κάποια ποσότητα από τα δύο νομίσματα και να τα δώσει στο πρωτόκολλο στην ίδια αναλογία που βρίσκονται στο LP, ώστε να μην μεταβάλλει την τιμή. Έπειτα, συνήθως το πρωτόκολλο του επιστρέφει ένα άλλο νόμισμα, το οποίο αντιπροσωπεύει το ποσοστό της συνολικής ρευστότητας που κατέχει ο χρήστης, στο συγκεκριμένο LP.

Όταν κάποιος παρέχει ρευστότητα σε ένα πρωτόκολλο, υπάρχει ο λεγόμενος κίνδυνος της προσωρινής απώλειας (Impermanent Loss). Κάθε φορά που ο χρήστης θέλει να πάρει πίσω τα αρχικά του νομίσματα, τότε δίνει πίσω στο πρωτόκολλο αυτά τα LP νομίσματα και του επιστρέφονται κάποια νομίσματα, ανάλογα με την τρέχουσα αναλογία του  $x$  και  $y$ . Μειώνοντας την συνολική ρευστότητα  $k$ , η επιθυμία είναι η τιμή και η αναλογία να παραμείνουν πάλι σταθερές, όμως η αναλογία πολλές φορές είναι διαφορετική από την αρχική. Υπάρχουν λοιπόν οι εξής τρεις περιπτώσεις:

- **Η αναλογία των  $x$  και  $y$  και άρα η τιμή είναι ακριβώς η ίδια με την κατάσταση όπου ο χρήστης πρόσφερε ρευστότητα στο LP:** Σε αυτή την περίπτωση, ο χρήστης θα πάρει πίσω την ίδια ακριβώς ποσότητα των νομισμάτων, με αυτή που πρόσφερε.
- **Υπάρχουν περισσότερα  $x$  από  $y$  στο LP από όταν ο χρήστης πρόσφερε ρευστότητα και άρα η τιμή του  $x$  σε σχέση με το  $y$  έχει μειωθεί:** Σε αυτή την περίπτωση, ο χρήστης θα πάρει πίσω περισσότερα νομίσματα  $x$  και λιγότερα  $y$ .
- **Υπάρχουν λιγότερα  $x$  από  $y$  στο LP από όταν ο χρήστης πρόσφερε ρευστότητα και άρα η τιμή του  $x$  σε σχέση με το  $y$  έχει αυξηθεί:** Σε αυτή την περίπτωση, ο χρήστης θα πάρει πίσω λιγότερα νομίσματα  $x$  και περισσότερα  $y$ .

Στις δύο τελευταίες περιπτώσεις, παρατηρείται το φαινόμενο της προσωρινής απώλειας, το οποίο ονομάζεται έτσι επειδή ο χρήστης καταλήγει να παίρνει πίσω πάντα περισσότερα νομίσματα από το νόμισμα του οποίου η τιμή μειώθηκε σε σχέση με το άλλο ενώ αν απλά κρατούσε τα νομίσματα αυτά στο πορτοφόλι του, θα είχαν περισσότερη νομισματική αξία.

Είναι δυνατό επίσης, να υπολογιστεί και να γίνει αναπαράσταση της ποσοτικής αυτής απώλειας [42]. Αν οριστεί ως  $z$  η ποσοστιαία μεταβολή στην τιμή του  $x$  ως προς το  $y$ , δηλαδή  $z = P_{x \text{ τελικό}}/P_{x \text{ αρχικό}}$ , τότε η ποσοστιαία απώλεια από αυτή τη μεταβολή στην τιμή του  $x$  υπολογίζεται από τον παρακάτω τύπο:

$$IL(z) = \frac{2\sqrt{z}}{1+z} - 1$$

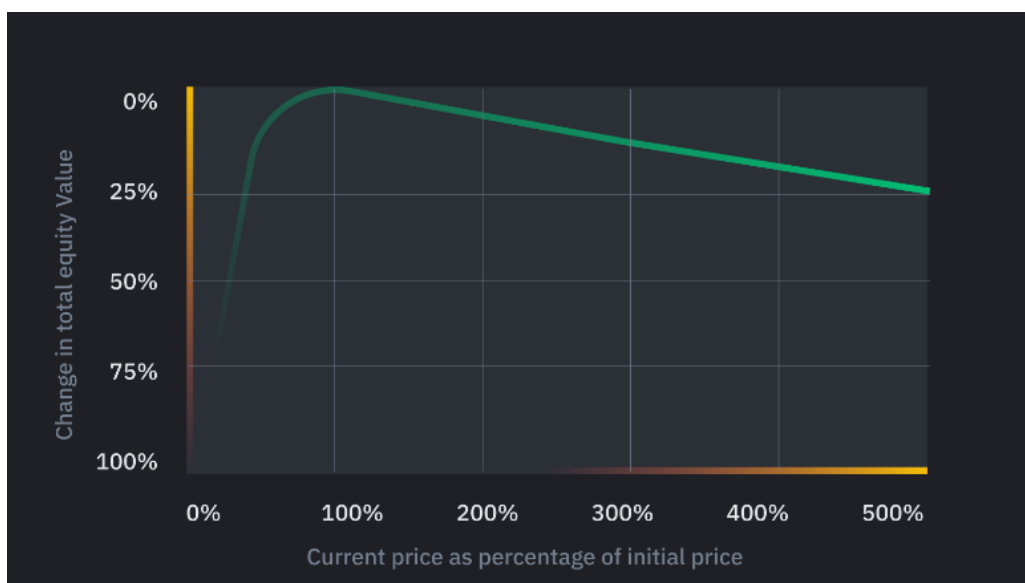


Figure 5. Το φαινόμενο της προσωρινής απώλειας σε σχέση με την αύξηση της τιμής

Λεπτομέρειες για τον υπολογισμό αυτού του τύπου μπορούν να βρεθούν στη βιβλιογραφία, η οποία παρατίθεται στις τελευταίες σελίδες της παρούσας εργασίας.

Προκύπτει όμως το ερώτημα, γιατί τότε κάποιος να δώσει τα νομίσματά του ως ρευστότητα σε ένα πρωτόκολλο, αντί να τα κρατήσει στο πορτοφόλι του, αφού υπάρχει αυτός ο κίνδυνος να χάσει κάποια αξία από αυτά. Αυτός ο κίνδυνος αντισταθμίζεται από κάποια κίνητρα που παρέχει το κάθε πρωτόκολλο, ώστε να ενθαρρύνει τους χρήστες για την παροχή ρευστότητας. Για παράδειγμα κάθε συναλλαγή στο Uniswap, έχει έναν επιπλέον φόρο για τον χρήστη και ο οποίος διανέμεται ως ανταμοιβή στους χρήστες που παρέχουν ρευστότητα στο συγκεκριμένο LP. Αυτό διανέμεται αναλογικά με το ποσοστό της συνολικής ρευστότητας που κατέχει ο κάθε χρήστης στο LP, αν δηλαδή κάποιος παρείχε το 20% της συνολικής ρευστότητας σε ένα LP, τότε θα έπαιρνε ως ανταμοιβή το 20% των συνολικών φόρων από κάθε συναλλαγή που γίνεται για το συγκεκριμένο ζευγάρι νομισμάτων. Κάποια άλλα πρωτόκολλα, όπως το Sushiswap, δίνουν επίσης ως κίνητρο κάποια δικά τους νομίσματα (π.χ. Sushi), ως ανταμοιβή για αυτούς που παρέχουν ρευστότητα στο πρωτόκολλό τους.

Τέλος, μπορεί κάποιος να αναρωτηθεί πώς όλα αυτά τα αυτοματοποιημένα αποκεντρωμένα ανταλλακτήρια καταφέρνουν να διατηρούν σταθερές τιμές μεταξύ τους. Πώς δηλαδή στην πράξη, η τιμή των ίδιων νομισμάτων σε διαφορετικά ανταλλακτήρια είναι η ίδια ενώ πραγματοποιούνται διαφορετικές συναλλαγές κι αυτά δεν επικοινωνούν κάπως μεταξύ τους; Η απάντηση βρίσκεται στους επενδυτές οι οποίοι αναζητούν κάποιο κέρδος. Αν η τιμή ενός νομίσματος, για παράδειγμα του ETH σε USD είναι 10% πιο ψηλά από κάποιο άλλο ανταλλακτήριο και κάποιος το παρατηρήσει αυτό, μπορεί να αγοράσει κάποια ποσότητα από ETH από το δεύτερο ανταλλακτήριο και να την πουλήσει στο πρώτο 10% πιο πάνω, και να βγάλει κέρδος μέχρι η τιμή των δύο ανταλλακτηρίων να εξισορροπηθεί. Αυτή η πράξη είναι γνωστή και ως arbitrage [43] και είναι ο λόγος που αν και βραχυπρόθεσμα οι τιμές των νομισμάτων στα διάφορα ανταλλακτήρια μπορεί να είναι διαφορετικές, μακροπρόθεσμα συγκλίνουν.

Με την ύπαρξη αυτών των AMM λοιπόν, οι διάφοροι χρήστες μπορούν να ανταλλάσσουν τα νομίσματά τους πλήρως αποκεντρωμένα, χωρίς κάποιο κεντρικό φορέα. Χρειάζεται δηλαδή να εμπιστεύονται μόνο ένα AMM πρόγραμμα, που είναι πλήρως διαφανές και δημόσιο, στο blockchain έναντι ενός ιδιωτικού σέρβερ.

Έχοντας κατανοήσει όλα τα παραπάνω, ακολουθεί τώρα η λειτουργία του DMT Automated Market Maker και ο τρόπος που επιτυγχάνει μακροπρόθεσμη σταθερότητα στην τιμή των νομισμάτων του.

### **3.7. To Dollar Market Token AMM**

Η σταθερότητα στην τιμή του DMT νομίσματος βασίζεται κατά κύριο λόγο στο αποκεντρωμένο ανταλλακτήριο, που βρίσκεται στο πυρήνα του πρωτοκόλλου. Αυτό το ανταλλακτήριο ακολουθεί τις βασικές αρχές των AMM της προηγούμενης ενότητας και εισάγει κάποιες επιπλέον λειτουργίες, ώστε να διατηρεί την σταθερότητα στις τιμές.

Πιο συγκεκριμένα το DMT AMM έχει τα εξής χαρακτηριστικά:

- Περιέχει ένα ζευγάρι από ρευστότητα (LP) μεταξύ DMT/USD.
- Ακολουθεί την εξίσωση  $x * y = k$ , η οποία περιγράφεται στην προηγούμενη ενότητα, για την προσαρμογή της τιμής και της συνολικής ποσότητας των αγαθών, όταν οι χρήστες ανταλλάσσουν σε αυτό.
- Αρχικοποιείται με  $10^{15}$  USD και DMT νομίσματα και άρα με αρχική τιμή  $1 \text{ DMT} = 1 \text{ USD}$ .
- Περιέχει ένα θησαυροφυλάκιο (treasury), στο οποίο αποθηκεύει τα επιπλέον USD, όταν η προσφορά τους αυξάνεται πάνω από ένα όριο, ώστε να διατηρήσει σταθερές τιμές μεταξύ του USD και του DMT.
- Ένα βιβλίο χρέους, όπου αποθηκεύει το συνολικό χρέος του πρωτοκόλλου για κάθε χρήστη. Όπως θα αναλυθεί στην επόμενη ενότητα, όταν η ζήτηση για DMT μειώνεται και η τιμή του πέφτει κάτω από ένα ορισμένο σημείο, το πρωτόκολλο διανέμει ομόλογα νομίσματα σε μορφή χρέους, ώστε να αυξήσει την τρέχουσα προσφορά από USD.

Ακολουθεί η διαδικασία με την οποία το πρωτόκολλο συνδυάζει όλα τα παραπάνω, ώστε να διατηρεί σταθερή τιμή στην ισοτιμία του DMT/USD.

### 3.8. Πώς το πρωτόκολλο του DMT επιτυγχάνει σταθερότητα στην ισοτιμία

Όπως αναφέρθηκε στη προηγούμενη ενότητα, ο πυρήνας του πρωτοκόλλου βασίζεται στο DMT AMM. Μπορεί να θεωρηθεί το DMT AMM και ως η Κεντρική Τράπεζα μιας χώρας [44], όπου κάποιος παρατηρεί την τρέχουσα ζήτηση στο DMT και προσαρμόζει την τρέχουσα νομισματική πολιτική, με βάση αυτή, ώστε να πετύχει μακροπρόθεσμα μια σταθερή ισοτιμία μεταξύ DMT και USD. Αυτές οι αποφάσεις γίνονται πλήρως αποκεντρωμένα, με βάση έναν αλγόριθμο, ο οποίος τρέχει στο blockchain και ο οποίος είναι πλήρως προσβάσιμος και διαφανής σε όλους.

Ακολουθεί η λειτουργία του πρωτοκόλλου κάθε φορά που γίνεται μια ανταλλαγή στο AMM του DMT πρωτοκόλλου:

- Αρχικά, το πρωτόκολλο υπολογίζει τα νομίσματα που οφείλει στον χρήστη, σύμφωνα με την  $x * y = k$  εξίσωση και πραγματοποιεί την συναλλαγή, μεταφέροντάς του τα επιθυμητά νομίσματα.
- Από την προηγούμενη ενότητα είναι γνωστό ότι αυτή η ενέργεια έχει ως αποτέλεσμα την αύξηση της ποσότητας ενός αγαθού μέσα στη δεξαμενή ρευστότητας LP και την μείωση του άλλου, με αποτέλεσμα την αλλαγή της ισοτιμίας τους.
- Το πρωτόκολλο έπειτα υπολογίζει την μελλοντική τιμή του DMT, μετά από αυτήν την συναλλαγή ως προς το USD και ελέγχει αν βρίσκεται μεταξύ του εύρους  $1 \text{ USD} \pm \epsilon$ . Το  $\epsilon$  είναι μια παράμετρος του πρωτοκόλλου και μπορεί να προσαρμοστεί, αλλάζοντας το πόσο γρήγορα αντιδράει το πρωτόκολλο σε μεταβολές της τιμής. Όσο μικρότερο το  $\epsilon$ , τόσο πιο γρήγορα αντιδράει το πρωτόκολλο σε αποκλίσεις της ισοτιμίας. Σε αυτό το παράδειγμα έστω ότι το  $\epsilon$  είναι 0.05.
- Υπάρχουν τρεις περιπτώσεις:

- **Η υπολογισμένη τιμή του 1 DMT είναι μεταξύ του  $\pm$  εύρους  $\epsilon$ :** Σε αυτή την περίπτωση, το πρωτόκολλο θεωρεί ότι η ισοτιμία βρίσκεται ακόμη σε επιθυμητά επίπεδα και δεν πραγματοποιεί κάποια επιπλέον ενέργεια.
- **Η υπολογισμένη τιμή του 1 DMT είναι μεγαλύτερη από  $1 \text{ USD} + \epsilon$ :** Αυτό συμβαίνει όταν ένας χρήστης ανταλλάσσει τα USD του για DMT, μειώνοντας την ποσότητά τους στη δεξαμενή ρευστότητας και αυξάνοντας την ποσότητα των USD. Στην περίπτωση κατά την οποία το πρωτόκολλο θα πρόσθετε αυτά τα καινούργια USD στο LP, η τιμή θα ξεπερνούσε την τιμή του  $1 \text{ USD} + \epsilon$ . Το πρωτόκολλο άρα χρειάζεται να υλοποιήσει μια πολιτική, ώστε η ποσότητα από USD να επανέλθει στην επιθυμητή. Αυτό που κάνει το πρωτόκολλο, είναι ότι αντί να προσθέσει αυτά τα επιπλέον USD στη δεξαμενή ρευστότητάς του, τα αποθηκεύει σε ένα θησαυροφυλάκιο ώστε να τα χρησιμοποιήσει, όπως θα αναφερθεί αργότερα.
- **Η υπολογισμένη τιμή του 1 DMT είναι μικρότερη από  $1 \text{ USD} - \epsilon$ :** Αυτό σημαίνει ότι η τρέχουσα ζήτηση για DMT είναι μικρότερη από τη ζήτηση του USD, με αποτέλεσμα να υπάρχει περισσότερη ποσότητα από DMT σε σχέση με USD, ως ρευστότητα. Αρχικά, για να αυξήσει την ποσότητα από USD, προσθέτει στην LP τα USD, όπου έχει αποθηκευμένα στο θησαυροφυλάκιο από την προηγούμενη φάση της διαστολής. Αν τα αποθηκευμένα USD τελειώσουν και η τιμή βρίσκεται ακόμη πιο χαμηλά από την επιθυμητή, το πρωτόκολλο δημιουργεί και διανέμει ομόλογα DebtNFT στους ενδιαφερόμενους επενδυτές και τα εισάγει στην Ουρά Ομολόγων του, μέχρι η ποσότητα από USD να φτάσει την επιθυμητή.
- Το πρωτόκολλο αρχίζει να ξεπληρώνει τα ομόλογα από την Ουρά Ομολόγων, μέσω των USD που μαζεύει στο θησαυροφυλάκιο, όταν η ζήτηση και η τιμή του DMT αρχίζουν να ανακάμπτουν, με προτεραιότητα από το παλαιότερο στο νεότερο. Με αυτό τον τρόπο επίσης, ενθαρρύνει τους επενδυτές να αγοράσουν τα ομόλογα, όσο πιο σύντομα γίνεται, καθώς όσο πιο νωρίς τα αγοράσουν, τόσο πιο νωρίς θα ξεπληρωθούν.

Η Ουρά Ομολόγων είναι ανάλογη του δημόσιου χρέους. Ακριβώς όπως το DMT πρωτόκολλο δημιουργεί ομόλογα, τα οποία παραμένουν στην Ουρά Ομολόγων μέχρι να ξεπληρωθούν, έτσι και η κυβέρνηση προσφέρει κρατικά ομόλογα, τα οποία προστίθενται στο δημόσιο χρέος μέχρι να ξεπληρωθούν. Επίσης, το πρωτόκολλο δίνει ένα επιπλέον κίνητρο στους χρήστες για την αγορά ομολόγων DebtNFT έναντι DMT νομισμάτων, σε περιόδους μειωμένης ζήτησης, υπολογίζοντας το ωφελούμενο χρέος από την τιμή του DMT σε USD την στιγμή της δημιουργίας του, μαζί με μια επιπλέον ανταμοιβή  $+5\%$ . Έτσι, κάθε χρήστης που βοηθάει στην επαναφορά της τιμής του DMT, όταν αυτή βρίσκεται κάτω από το  $1 \text{ USD}$  δίνοντας τα USD του για DebtNFT, θα επωφελείται αρχικά από την αυξημένη τιμή του DMT κι επιπροσθέτως από την επιπλέον ανταμοιβή.

Μέσω της εφαρμογής των παραπάνω πολιτικών και της μεταβολής της τρέχουσας προσφοράς από USD, αναλόγως της τρέχουσας τιμής, το πρωτόκολλο καταφέρνει να διατηρεί μια σταθερή ισοτιμία του DMT με το USD.

### 3.9. Βελτιώσεις

Αν και το DMT πρωτόκολλο καταφέρνει, όπως θα αναφερθεί στην επόμενη ενότητα, να διατηρεί σταθερή την ισοτιμία μακροπρόθεσμα, υπάρχει ακόμη χώρος για βελτίωση. Οι παρακάτω ιδέες δεν υλοποιήθηκαν στην παρούσα εργασία λόγω πολυπλοκότητας, καθώς ο κύριος σκοπός ήταν η παρουσίαση της σταθερότητας των τιμών. Σε αυτή την ενότητα, θα παρουσιαστούν κάποιες πιθανές βελτιώσεις, οι οποίες θα μπορούσαν να εφαρμοστούν για την αποφυγή πιθανών προβλημάτων και την βελτίωση της αποτελεσματικότητας του πρωτοκόλλου.

#### 3.9.1. Ημερομηνία λήξης των ομολόγων

Στην παρούσα υλοποίηση, κάθε ομόλογο NFT που βρίσκεται στην Ουρά Ομολόγων, παραμένει μέσα αυτήν μέχρι την στιγμή που θα ξεπληρωθεί πλήρως. Ένα μειονέκτημα αυτής της μεθόδου είναι ότι μπορεί να δημιουργηθεί μια κατάσταση κατά την οποία η Ουρά Ομολόγων είναι τόσο μεγάλη, όπου οι επενδυτές δεν έχουν πλέον συμφέρον να αγοράσουν νέα ομόλογα, καθώς αυτά θα τοποθετηθούν στο τέλος της ουράς και το ρίσκο είναι μεγαλύτερο από την πιθανή ανταμοιβή που θα λάβουν. Όσο μεγαλύτερη γίνεται η Ουρά των Ομολόγων, τόσο περισσότερος χρόνος απαιτείται για νέα ομόλογα που βρίσκονται στο τέλος της ουράς ώστε να εξαργυρωθούν. Αυτό έχει ως αποτέλεσμα την πτώση των τιμών των νέων ομολόγων καθώς οι επενδυτές περιμένουν μεγαλύτερη απόδοση για τον επιπλέον χρόνο και ρίσκο που λαμβάνουν. Αν όμως η τιμή των καινούργιων ομολόγων πέσει στο μηδέν, αυτό σημαίνει ότι κανένας δεν θέλει να ανταλλάξει τα USD νομίσματα για ομόλογα και το σύστημα δεν μπορεί να μειώσει άλλο την USD προσφορά. Για να αποτραπεί μια τέτοια περίπτωση, κάθε ομόλογο το οποίο έχει παραμείνει για περισσότερο από 5 χρόνια στην ουρά θεωρείται άκυρο, ακόμη κι αν δεν έχει εξαργυρωθεί ακόμα. Επιλέχθηκε η διάρκεια των 5 χρόνων, επειδή θεωρήθηκε ότι αυτή θα παρέχει τη μεγαλύτερη σταθερότητα στο πρωτόκολλο, ακόμη και σε περιστάσεις έντονων μεταβολών της τιμής.

Αυτό όμως συνεπάγεται και μειονεκτήματα. Η εισαγωγή μιας ημερομηνίας μετά από την οποία τα ομόλογα δεν μπορούν να εξαργυρωθούν, καθιστά αυτή την επένδυση πιο ριψοκίνδυνη, με συνέπεια την γενική πτώση στις τιμές των ομολόγων. Το πιο σημαντικό όμως είναι ότι σε κρίσιμες περιόδους, κατά τις οποίες η ζήτηση για DMT μπορεί να είναι μειωμένη για μεγάλα χρονικά διαστήματα, η ύπαρξη μιας ημερομηνίας λήξης για τα παλαιότερα ομόλογα, βοηθάει στην γρηγορότερη επαναφορά της ζήτησης στα αρχικά επίπεδα. Για παράδειγμα, αν η ζήτηση του DMT έπεφτε δραστικά μέσα σε έναν χρόνο και δεν επανερχόταν στα επόμενα 5 χρόνια, ώστε να ξεπληρώσει όλα τα ομόλογα που δημιουργήθηκαν τον 1<sup>ο</sup> χρόνο, τότε αυτά τα ομόλογα απλά θα έληγαν. Στην αντίθετη περίπτωση, τα ομόλογα του πρώτου χρόνου θα παρέμεναν στην ουρά μέχρι να ξεπληρωθούν, αποθαρρύνοντας νέους επενδυτές από το να αγοράσουν νέα ομόλογα, λόγω του συνολικού μεγέθους της Ουράς Ομολόγων, με αποτέλεσμα η ζήτηση να μειώνεται ακόμη περισσότερο και ούτω κάθε εξής.

Επίσης, γίνεται κατανοητό όμως, ότι η εισαγωγή μιας ημερομηνίας λήξης και η μείωση του συνολικού μήκους της Ουράς Ομολόγων, έχει ως αποτέλεσμα μια γενική αύξηση στις τιμές των νέων ομολόγων, σε σχέση με την κατάσταση χωρίς την ύπαρξη ημερομηνίας λήξης, καθώς



οι νέοι επενδυτές πρέπει να λάβουν υπόψη και το επιπλέον ρίσκο της περίπτωσης κατά την οποία το ομόλόγό τους λήγει και δεν ξεπληρώνονται ποτέ. Επομένως, η χρήση ημερομηνίας λήξης αφορά ουσιαστικά μια “θυσιά”, ώστε το πρωτόκολλο να διατηρεί περισσότερη σταθερότητα σε κρίσιμες περιόδους, σε βάρος μικρών ασταθειών σε πιο ήπιες περιόδους. Αν συγκριθεί για μια ακόμη φορά η λειτουργία του DMT πρωτοκόλλου με αυτήν της Κεντρικής Τράπεζας, τότε είναι δυνατό να διαπιστωθεί ότι η ημερομηνία λήξης προσφέρει ισορροπία μεταξύ υψηλότερου κόστους δανεισμού στο παρόν (με τη μορφή φθηνότερων ομολόγων, όταν η Ουρά Ομολόγων είναι μικρή) και χαμηλότερου κόστους δανεισμού, όταν το πρωτόκολλο το χρειάζεται πραγματικά (με τη μορφή ακριβότερων ομολόγων και μεγαλύτερων ανταμοιβών).

Τέλος, αντί για την εισαγωγή μιας ημερομηνίας λήξης στην Ουρά Ομολόγων, θα μπορούσε να εφαρμοστεί ένας αλγόριθμος, ο οποίος προσαρμόζει την μελλοντική ανταμοιβή από ένα ομόλογο τη στιγμή της δημιουργίας του, με βάση το μήκος της ουράς. Όσο μεγαλύτερη είναι η ουρά και άρα το ρίσκο για έναν επενδυτή προκειμένου να επενδύσει σε ένα νέο ομόλογο, τόσο μεγαλύτερη θα είναι και η μελλοντική ανταμοιβή του. Αυτό επίσης, για παρόμοιους λόγους με αυτούς της ημερομηνίας λήξης, πετυχαίνει καλύτερα αποτελέσματα από τη χρήση σταθερών ανταμοιβών, ανεξαρτήτως του μεγέθους της ουράς, καθώς δίνει το ανάλογο κίνητρο στους επενδυτές ώστε να αγοράσουν νέα ομόλογα με βάση το τρέχον ρίσκο τους.

### **3.9.2. Πώληση ομολόγων μέσω ανοιχτών δημοπρασιών**

Στην τρέχουσα υλοποίηση, όταν η ζήτηση από DMT μειωθεί αρκετά και το θησαυροφυλάκιο από USD είναι άδειο, η αγορά ομολόγων είναι ανοιχτή και μπορεί οποιοσδήποτε να αγοράσει πραγματοποιώντας μια συναλλαγή. Πιθανή βελτίωση σε αυτή τη μέθοδο, θα ήταν η διεξαγωγή και η πώληση νέων ομολόγων μέσω ανοιχτής δημοπρασίας μεταξύ των ενδιαφερόμενων αντί για την πώλησή τους στην ανοιχτή αγορά.

Ακολουθούν διευκρινίσεις σχετικά με τον τρόπο που θα μπορούσε να λειτουργήσει κάτι τέτοιο. Όταν η ζήτηση από DMT έχει μειωθεί σε σημείο που το πρωτόκολλο χρειάζεται να την επαναφέρει διανέμοντας ομόλογα, για να επιλέξει την τιμή των νέων ομολόγων το σύστημα μπορεί να εκτελέσει μια σειρά από ανοικτές δημοπρασίες, στις οποίες όλοι οι ενδιαφερόμενοι ορίζουν μια επιθυμητή τιμή και το ποσό των ομολόγων που θέλουν να αγοράσουν στην συγκεκριμένη τιμή. Για παράδειγμα, κάποιος μπορεί να ορίσει ότι θέλει να αγοράσει 100 ομόλογα για 0.9 USD το καθένα. Έπειτα, το σύστημα ταξινομεί όλες τις προσφορές που έλαβε με βάση την τιμή και υπολογίζει την τιμή εκκαθάρισης, τη μεγαλύτερη τιμή, δηλαδή, στην οποία όλα τα ομόλογα που θέλει να πουλήσει το πρωτόκολλο, θα αγορασθούν. Τέλος, διανέμει τα ομόλογα στην τιμή εκκαθάρισης, με προτεραιότητα από την υψηλότερη προσφερόμενη τιμή στη χαμηλότερη.

Παράδειγμα:

- Υποτίθεται ότι το σύστημα θέλει να πουλήσει 100 ομόλογα συνολικά, ώστε να επαναφέρει την τιμή.
- Υποτίθεται επίσης ότι υπάρχουν 3 προσφορές: Μια προσφορά για 80 ομόλογα προς 0.8 USD το καθένα, μια για 80 ομόλογα προς 0.6 USD το καθένα και μια για 80 ομόλογα προς 0.4 USD το καθένα.

- Το σύστημα υπολογίζει την τιμή εκκαθάρισης, η οποία στην προκειμένη περίπτωση ισούται με 0.6 USD.
- Το σύστημα έπειτα, διανέμει τα ομόλογα με σειρά προτεραιότητας, αναλόγως της προσφερόμενης τιμής, στην τιμή εκκαθάρισης. Ο πρώτος χρήστης λοιπόν, θα πάρει 80 ομόλογα και θα δώσει σε αντάλλαγμα  $80 * 0.6 = 48$  USD νομίσματα, και ο δεύτερος ενδιαφερόμενος θα λάβει 20 ομόλογα με αντάλλαγμα  $20 * 0.6 = 12$  νομίσματα. Ο τρίτος δεν θα πάρει κανένα ομόλογο καθώς η προσφερόμενη τιμή του ήταν πολύ χαμηλή.

Μια τέτοια μέθοδος δίνει καλύτερα αποτελέσματα από την μέθοδο της ελεύθερης αγοράς που χρησιμοποιήθηκε, καθώς παρέχει σε όλους τους ενδιαφερόμενους τις ίδιες πιθανότητες ώστε να αγοράσουν τα ομόλογα που θέλουν, στην επιθυμητή τους τιμή. Στην αντίθετη περίπτωση της ελεύθερης αγοράς, σε περιόδους όπου η τιμές των ομολόγων είναι αρκετά ελκυστικές και η ζήτησή τους είναι μεγάλη, πολλά από τα ομόλογα θα καταλήξουν σε bots που ελέγχουν συνεχώς για ευκαιρίες και πολλοί ενδιαφερόμενοι δεν θα καταφέρουν να πάρουν. Τέλος, το πρωτόκολλο μπορεί να ορίσει και ένα τεχνητό κατώτατο όριο στην τιμή εκκαθάρισης, ώστε να διασφαλίσει ότι ο δανεισμός αυτός δεν ξεπερνάει κάποια τιμή, η οποία θα επηρεάσει αρνητικά τη μελλοντική σταθερότητα του συστήματος.

Επειδή η παρούσα εργασία έχει κύριο σκοπό την εκπαίδευση και την έρευνα όσον αφορά στα σταθερά κρυπτονομίσματα, για λόγους απλότητας δεν εφαρμόστηκαν τα παραπάνω, τα οποία είναι ύψιστης σημασίας σε ανταγωνιστικά περιβάλλοντα του πραγματικού κόσμου. Στην επόμενη ενότητα θα παρουσιαστεί η μέθοδος που ακολουθήθηκε για την διάγνωση του DMT αλγορίθμου καθώς και τα αποτελέσματα στα οποία κατέληξε.

## 4. Πειράματα & Αποτελέσματα

### 4.1. Μεθοδολογία

Ο αλγόριθμος του DMT υλοποιήθηκε στη γλώσσα Solidity [45]. Η γλώσσα Solidity είναι μια από της πιο δημοφιλείς γλώσσες προγραμματισμού για την ανάπτυξη blockchain εφαρμογών, οι οποίες εκτελούνται με βάση το EVM μοντέλο [46]. Αυτό σημαίνει ότι τα προγράμματα που είναι γραμμένα στη γλώσσα Solidity μπορούν να εκτελεστούν από κάθε blockchain που ακολουθεί το EVM μοντέλο για την εκτέλεση των προγραμμάτων, όπως είναι τα Ethereum, Binance Smart Chain, Avalanche και Fantom. Η γλώσσα παρουσιάζει κοινά χαρακτηριστικά με τις κλασικές αντικειμενοστραφείς γλώσσες προγραμματισμού, όπως είναι η Java και C# αλλά και με γλώσσες όπως η JavaScript ή C++. Για την ανάπτυξη και δημοσίευση του προγράμματος στο blockchain χρησιμοποιήθηκε επίσης το εργαλείο Truffle [47], το οποίο είναι συλλογή χρήσιμων εργαλείων για την ανάπτυξη και τη δημοσίευση των εφαρμογών στο blockchain.

Τα πιο σημαντικά εργαλεία που παρέχει είναι τα εξής:

- Solidity Compiler για την μεταγλώττιση του κώδικά μας από τη γλώσσα Solidity σε εντολές, τις οποίες το εικονικό μηχάνημα του Ethereum (EVM) μπορεί να εκτελέσει.
- Εργαλεία για εύκολη δημοσίευση των προγραμμάτων σε οποιοδήποτε blockchain δίκτυο.
- Εργαλεία για την ανάπτυξη αυτοματοποιημένων διαγνωστικών ελέγχων ώστε να υπάρχει βεβαιότητα ότι το πρόγραμμα εκτελείται σωστά πριν δημοσιευτεί στο blockchain.
- Δυνατότητα δημοσίευσης των προγραμμάτων σε ένα τοπικό blockchain για τον καλύτερο έλεγχο τους.

Επίσης, το πρωτόκολλο δημοσιεύτηκε στο blockchain του BSC Testnet Network. Πρόκειται για ένα δημόσιο δοκιμαστικό δίκτυο blockchain του BSC, όπου οι χρήστες μπορούν να δημοσιεύσουν τα προγράμματά τους και να τα ελέγξουν πριν τα δημοσιεύσουν στο BSC. Το BSC, από τα αρχικά Binance Smart Chain, πρόκειται για ένα από τα πιο δημοφιλή blockchain δίκτυα σήμερα. Δημιουργήθηκε από το Binance, το οποίο είναι ένα από τα πιο μεγάλα και δημοφιλή ανταλλακτήρια σε όλο τον κόσμο [48]. Έχει πολλά κοινά χαρακτηριστικά με το Ethereum δίκτυο, καθώς λειτουργεί και αυτό με βάση ενός EVM μοντέλου κι επομένως όλα τα προγράμματα που έχουν γραφτεί για το δίκτυο του Ethereum μπορούν να τρέξουν επίσης και στο BSC και αντιστρόφως. Επιλέχθηκε αυτό το δίκτυο λόγω των γρήγορων ταχυτήτων του και επειδή τα κόστη των συναλλαγών του είναι συνήθως πολύ μικρότερα από αυτά του Ethereum.

Για την διεξαγωγή των πειραμάτων, αρχικά εκτελέστηκε μια σειρά από απλούς ελέγχους, ώστε να επιβεβαιωθεί ότι το πρωτόκολλο αντιδρά σύμφωνα με τις προδιαγραφές του πρωτοκόλλου, σε κάθε στάδιο του αλγορίθμου. Έπειτα, μελετήθηκαν κάποια παραδείγματα συναλλαγών από τον πραγματικό κόσμο και στη συνέχεια μέσω Python υλοποίησα μια σειρά από μοντέλα συναλλαγών που ακολουθούν τα δεδομένα από το πραγματικό κόσμο. Με αυτό τον τρόπο, παρατηρήθηκε ο τρόπος με τον οποίο αντιδρά το πρωτόκολλο, όταν έρχεται αντιμέτωπο με

πραγματικά δεδομένα. Κατά τη διάρκεια των πειραμάτων καταγράφηκαν όλες οι αλλαγές στα δεδομένα του προγράμματος, μετά από την εκτέλεση κάθε συναλλαγής και αποθηκεύτηκαν σε ξεχωριστά txt και excel αρχεία. Στη συνέχεια πραγματοποιήθηκε επεξεργασία αυτών των δεδομένων μέσω και δημιουργήθηκαν τα αντίστοιχα διαγράμματα για την καλύτερη κατανόηση τους.

Το τελευταίο βήμα ήταν η επαλήθευση του κώδικα μέσω του <https://testnet.bscscan.com/> ώστε να είναι δημόσιος και διαφανής για όλους στο blockchain. Ο κώδικας του πρωτοκόλλου είναι διαθέσιμος στο blockchain ακολουθώντας τον παρακάτω σύνδεσμο:

<https://testnet.bscscan.com/address/0x73ac4cdf67a456c448c453db40e595089df49be3#code>

Τέλος, ο κώδικας καθώς και τα αποτελέσματα από την εκτέλεση του είναι δημόσια, επίσης και στο [Github](#).

## 4.2. Αποτελέσματα

Αρχικά πραγματοποιήθηκε σειρά απλών ελέγχων για να επιβεβαιωθεί ότι το πρωτόκολλο συμπεριφέρεται σωστά σε κάθε στάδιο του αλγορίθμου. Στα παρακάτω διαγράμματα όταν η ισοτιμία είναι πάνω από 1, σημαίνει ότι 1 DMT κοστίζει λιγότερο από 1 USD και όταν είναι κάτω, σημαίνει ότι 1 DMT κοστίζει περισσότερο από 1 USD. Επίσης, ο όγκος των συναλλαγών που επιλέχθηκαν ισούται με το 1% της συνολικής ρευστότητας, ένα εξαιρετικά μεγάλο νούμερο σε σχέση με τις καθημερινές συναλλαγές. Με αυτό τον τρόπο επιβεβαιώνεται ταυτόχρονα ότι το πρωτόκολλο συμπεριφέρεται ορθά, ακόμη και στις καταστάσεις κατά τις οποίες πραγματοποιείται ένας μεγάλος όγκος συναλλαγών. Τέλος, σε αυτή τη φάση των ελέγχων τέθηκε απόκλιση ε ως 0.05.

Για το πρώτο πείραμα, ελέγχθηκε η συμπεριφορά του πρωτοκόλλου όταν πραγματοποιούνται συνεχόμενες συναλλαγές από USD σε DMT, δηλαδή όταν η ζήτηση για DMT είναι μεγαλύτερη από αυτή για USD. Πραγματοποιήθηκε λοιπόν μια σειρά από συνεχόμενες ανταλλαγές στο AMM από USD σε DMT. Τα αποτελέσματα από αυτές τις συναλλαγές φαίνονται στα παρακάτω διαγράμματα:

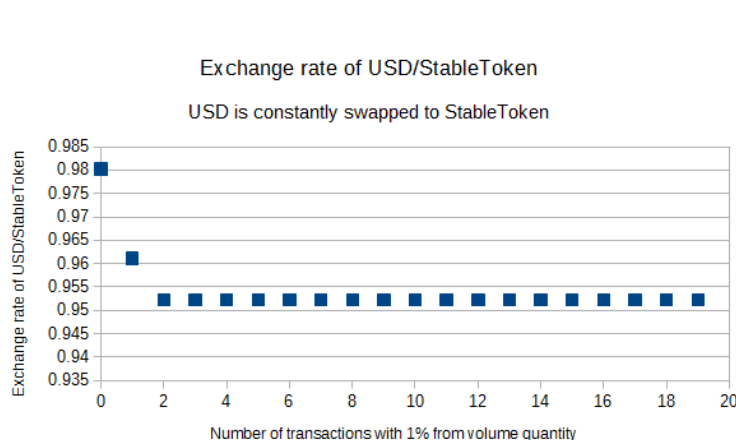


Figure 6. Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από USD σε DMT

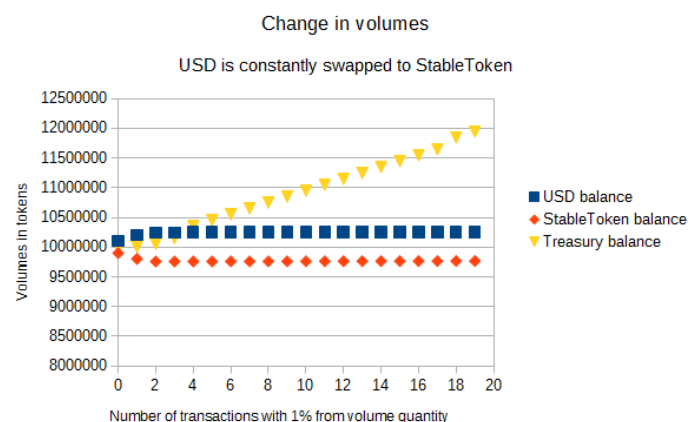


Figure 7. Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από USD σε DMT

Το πρώτο διάγραμμα δείχνει την μεταβολή της τρέχουσας ισοτιμίας καθώς πραγματοποιούνται οι συναλλαγές. Όπως παρατηρείται αρχικά η ισοτιμία πέφτει γρήγορα από το 1 που βρισκόταν, στο 0.95, αλλά έπειτα παραμένει σταθερή, παρ' όλο που οι συναλλαγές συνεχίζουν να αυξάνονται. Αυτό συμβαίνει επειδή το σημείο 0.95 είναι το σημείο της απόκλισης της ισοτιμίας που τέθηκε και όταν πάει να το ξεπεράσει το πρωτόκολλο εφαρμόζει μια πολιτική αποθήκευσης των νέων USD που λαμβάνει στο θησαυροφυλάκιο αντί για την αποθήκευσή τους στο LP. Με αυτό τον τρόπο αποτρέπει την μετέπειτα μεταβολή της τιμής καθώς η ποσότητα από USD στο LP δεν μεταβάλλεται, όπως είναι το αναμενόμενο.

Αυτό είναι πιο εμφανές από το δεύτερο διάγραμμα, το οποίο δείχνει τις μεταβολές στις ποσότητες των νομισμάτων σε βάθος χρόνου. Όπως παρατηρείται αρχικά η ποσότητα από USD στο LP αυξάνεται δραστικά και αναλογικά η ποσότητα από DMT μειώνεται. Μόλις όμως το πρωτόκολλο φτάσει την ισοτιμία 0.95, η ποσότητα από USD σταματάει να αυξάνεται και η ποσότητα από USD που βρίσκεται στο θησαυροφυλάκιο, που φαίνεται με την κίτρινη γραμμή, αρχίζει να αυξάνεται. Αυτό είναι με βάση τις προδιαγραφές του πρωτοκόλλου, το οποίο σε περιστάσεις αυξημένης ζήτησης DMT αρχίζει να συσσωρεύει την επιπλέον ποσότητα από USD στο θησαυροφυλάκιο, ώστε να σταματήσει την πτώση της ισοτιμίας.

Για τον επόμενο έλεγχο παρατηρήθηκε η συμπεριφορά του πρωτοκόλλου στην αντίθετη περίπτωση, όπου η ζήτηση για USD ξεπερνάει αυτήν για DMT. Από τον αλγόριθμο του πρωτοκόλλου είναι γνωστό ότι η συμπεριφορά του είναι διαφορετική, ανάλογα με το αν έχει αποθέματα από USD στο θησαυροφυλάκιο. Αρχικά ελέγχθηκε η περίπτωση σύμφωνα με την οποία το πρωτόκολλο έχει κάποια αποθέματα από USD στο θησαυροφυλάκιο, για να καλύψει την ζήτηση. Πραγματοποιήθηκε λοιπόν η αντίθετη διαδικασία με υποβολή συνεχόμενων ανταλλαγών από DMT σε USD, καθώς το θησαυροφυλάκιο είναι γεμάτο, καταγράφοντας τα αποτελέσματα. Τα παρακάτω διαγράμματα δείχνουν την συμπεριφορά του πρωτοκόλλου από αυτές τις συναλλαγές:

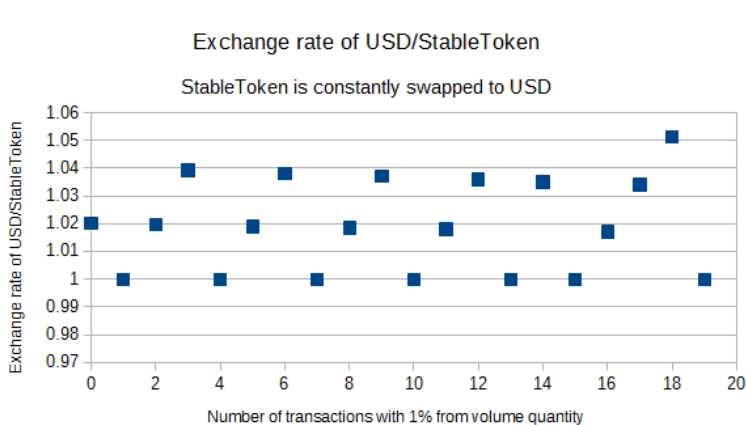


Figure 8. Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από DMT σε USD με θησαυροφυλάκιο

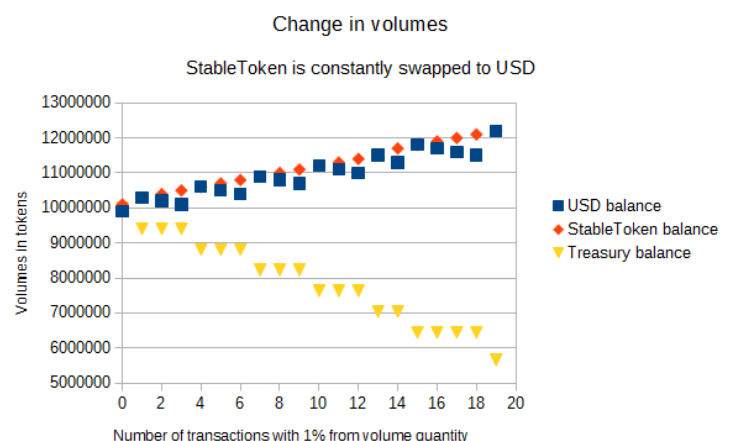


Figure 9. Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από DMT σε USD με θησαυροφυλάκιο

Όπως φαίνεται από το πρώτο διάγραμμα, η ισοτιμία ακολουθεί ένα επαναληπτικό μοτίβο, το οποίο αυξάνεται μέχρι την τιμή 1.05, που είναι το σημείο απόκλισης κι έπειτα επανέρχεται στο σημείο 1. Αυτό συμβαίνει επειδή στο σημείο απόκλισης το πρωτόκολλο αρχίζει να

απελευθερώνει τα USD που έχει αποθηκευμένα στο θησαυροφυλάκιο, μέχρι να επανέλθει η επιθυμητή ισοτιμία.

Αυτή η πτώση στη συνολική ποσότητα από USD που κατέχει το θησαυροφυλάκιο, φαίνεται καλύτερα στο δεύτερο διάγραμμα. Είναι εμφανές ότι καθώς αυξάνεται η ποσότητα από DMT στο LP, αυξάνεται ταυτόχρονα και η συνολική ποσότητα από USD αντί να μειώνεται, όπως σε ένα κλασσικό AMM. Αυτή η αύξηση στα USD προέρχεται από τα αποθέματα του θησαυροφυλακίου, τα οποία, όπως παρατηρείται από την κίτρινη γραμμή, μειώνονται αναλογικά ώστε να αντισταθμίσουν την αύξηση από DMT, όπως είναι και η αναμενόμενη συμπεριφορά του αλγορίθμου.

Για τον επόμενο έλεγχο παρατηρήθηκε ο τρόπος συμπεριφοράς του πρωτοκόλλου στην περίπτωση κατά την οποία η ζήτηση για USD είναι μεγαλύτερη από αυτή για DMT, αλλά τα αποθέματα στο θησαυροφυλάκιο έχουν τελειώσει. Το επόμενο διαγράμματα παρουσιάζουν τη συμπεριφορά του πρωτοκόλλου όταν πραγματοποιούνται συνεχόμενες συναλλαγές από DMT σε USD, αλλά τα αποθέματα USD του θησαυροφυλακίου είναι άδεια:

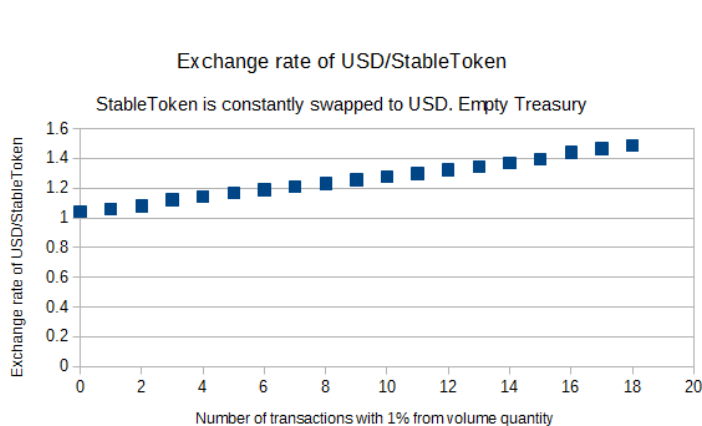


Figure 10. Μεταβολή της ισοτιμίας από συνεχόμενες ανταλλαγές από DMT σε USD χωρίς θησαυροφυλάκιο

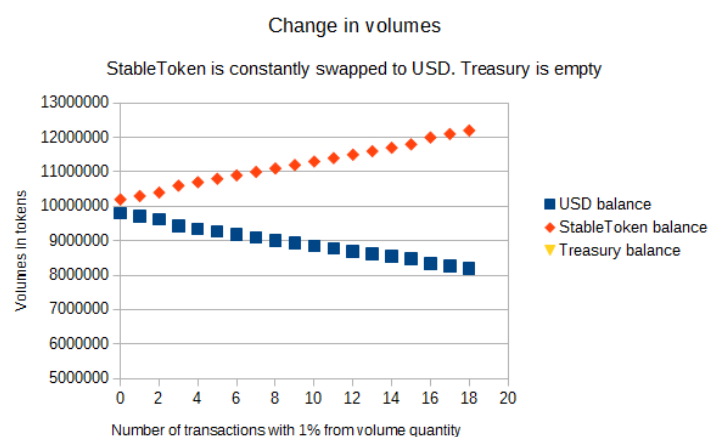


Figure 11. Μεταβολή της ποσότητας των νομισμάτων από συνεχόμενες ανταλλαγές από DMT σε USD χωρίς θησαυροφυλάκιο

Όπως φαίνεται από το πρώτο διάγραμμα, επειδή το πρωτόκολλο δεν έχει αποθέματα από USD στο θησαυροφυλάκιο για να αντισταθμίσει την αυξημένη ποσότητα από DMT, η ισοτιμία ξεπερνάει την τιμή απόκλισης 1.05 και συνεχίζει να αυξάνεται. Το δεύτερο διάγραμμα δείχνει την ποσότητα από USD στο LP να μειώνεται αναλογικά με την αύξηση από DMT καθώς δεν υπάρχει USD στο θησαυροφυλάκιο, το οποίο να μπορεί να απελευθερωθεί για να την αντισταθμίσει.

Όταν η ισοτιμία ξεπεράσει την τιμή απόκλισης, αρχίζουν να διανέμονται χρεωστικά ομόλογα NFT σε αντάλλαγμα με USD, για την επαναφορά της. Αυτή η διαδικασία παρουσιάζεται τελείως αποκομμένα από το προηγούμενο στάδιο, ώστε να φανεί πιο ξεκάθαρα η συμπεριφορά του πρωτοκόλλου, σε κάθε ξεχωριστό στάδιο. Σε ένα πραγματικό σενάριο, οι επενδυτές θα αγόραζαν πολύ πιο σύντομα τα χρεωστικά ομόλογα, επαναφέροντας την ισοτιμία ενώ βρισκόταν ακόμη κοντά στην τιμή απόκλισης. Παρακάτω φαίνονται τα αποτελέσματα από την αγορά και τη διανομή αυτών των ομολόγων:

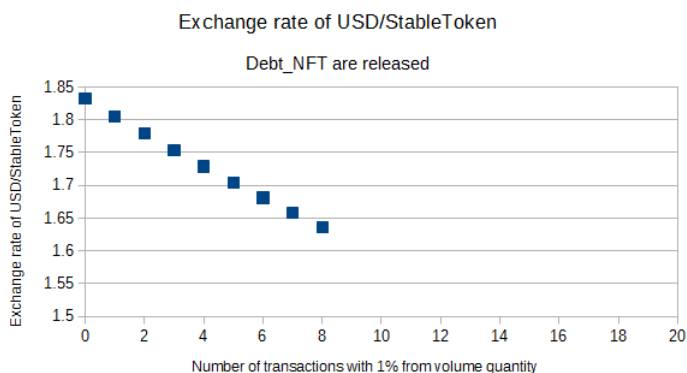


Figure 12. Μεταβολή της ισοτιμίας καθώς αγοράζονται Debt NFT

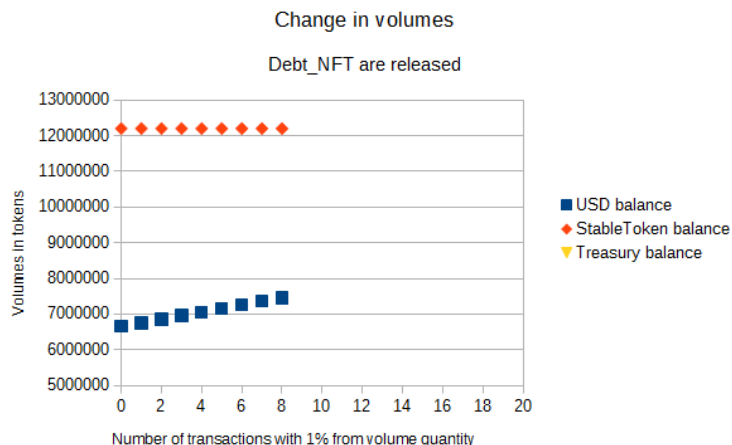


Figure 13. Μεταβολή της ποσότητας των νομισμάτων καθώς αγοράζονται Debt NFT

Όπως φαίνεται από το πρώτο διάγραμμα, καθώς το πρωτόκολλο αρχίζει να δημιουργεί και να διανέμει ομόλογα στους ενδιαφερόμενους, η ισοτιμία αρχίζει να μειώνεται και να συγκλίνει προς το σημείο της επιθυμητής ισοτιμίας. Από το δεύτερο διάγραμμα, φαίνεται ότι αυτή η διαδικασία επιτυγχάνεται λόγω της αύξησης των αποθεμάτων από USD στο AMM, μέσω της ανταλλαγής των Debt NFT για USD.

Τέλος, πραγματοποιήθηκαν κάποιοι έλεγχοι και παρατηρήθηκε ο τρόπος που αντιδρά το πρωτόκολλο, όταν η ζήτηση για DMT είναι και πάλι αυξημένη και η ισοτιμία πλησιάζει το σημείο απόκλισης ενώ υπάρχουν εκκρεμή ομόλογα. Τα αποτελέσματα από αυτόν τον έλεγχο φαίνονται καλύτερα στα δυο επόμενα διαγράμματα.

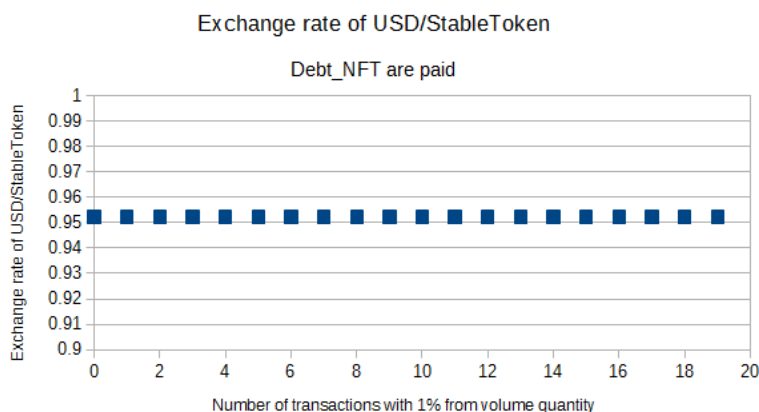


Figure 14. Μεταβολή της ισοτιμίας από συνεχιζόμενες ανταλλαγές από USD σε DMT με εκκρεμή ομόλογα

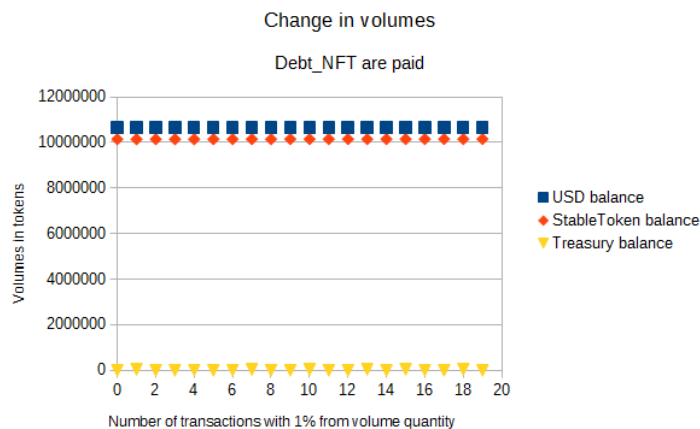


Figure 15. Μεταβολή της ποσότητας των νομισμάτων στο AMM από συνεχιζόμενες ανταλλαγές από USD σε DMT με εκκρεμή ομόλογα

Όπως αποτυπώνεται στα παραπάνω διαγράμματα, όταν η ισοτιμία φτάσει και πάλι στο σημείο απόκλισης 0.95 (διάγραμμα 1) και η ζήτηση για DMT είναι και πάλι περισσότερη από τη ζήτηση για USD, το πρωτόκολλο αντί να αποθηκεύσει τα επιπλέον USD στα αποθέματα του θησαυροφυλακίου του, όπως πριν, τα διανέμει στους κατόχους από τα εκκρεμή ομόλογα. Αυτό φαίνεται καλύτερα από το δεύτερο διάγραμμα, όπου σε αντίθεση με τον πρώτο έλεγχο που

πραγματοποιήθηκε το θησαυροφυλάκιο σε αυτή την περίπτωση παραμένει άδειο, καθώς τα επιπλέον USD διανέμονται στους κατόχους των ομολόγων. Όταν όλα τα ομόλογα ξεπληρωθούν και η Ουρά Ομολόγων είναι και πάλι άδεια, τότε το θησαυροφυλάκιο θα αρχίζει να γεμίζει και πάλι, όπως στην πρώτη περίπτωση. Από αυτούς τους ελέγχους γίνεται κατανοητό λοιπόν ότι είναι αδύνατο για το πρωτόκολλο να πέσει κάτω από την ισοτιμία 0.95, αλλά είναι δυνατό να αυξηθεί πάνω από το 1.05, σε περιστάσεις κατά τις οποίες δεν υπάρχει ζήτηση για τα ομόλογα NFT. Για να αποφευχθεί κάτι τέτοιο, δημιουργούνται ελκυστικά κίνητρα στους επενδυτές, ώστε να ανταλλάξουν τα USD τους, για ομόλογα.

Παρουσιάστηκε με αυτό τον τρόπο λοιπόν, ότι το πρωτόκολλο λειτουργεί ορθά, σύμφωνα με τις προδιαγραφές του, σε κάθε στάδιο. Τι γίνεται όμως σε πραγματικές καταστάσεις, όπου οι συναλλαγές είναι απρόβλεπτες και δεν ακολουθούν κάποιο σταθερό μοτίβο; Για να δοθεί επομένως μια ολοκληρωμένη εικόνα για την λειτουργία του πρωτοκόλλου, θα πρέπει επίσης να παρουσιαστεί η συμπεριφορά του σε καταστάσεις όπου οι συναλλαγές αντικατοπτρίζουν συναλλαγές από καταστάσεις του πραγματικού κόσμου. Για τον λόγο αυτό, κατασκευάστηκε ένα μοντέλο, το οποίο βασίζεται σε πραγματικά δεδομένα και στη συνέχεια παρατηρήθηκε η συμπεριφορά του πρωτοκόλλου αυτού, όταν έρχεται αντιμέτωπο με συναλλαγές αυτού του μοντέλου.

Το πρώτο μοντέλο από πραγματικά δεδομένα που χρησιμοποιήθηκε, προέρχεται από την μεταβολή στην ισοτιμία του USD/JPY, σε βάθος χρόνου. Στο επόμενο διάγραμμα παρουσιάζεται αυτή η μεταβολή από το διάστημα μεταξύ του 2018 και του 2021.

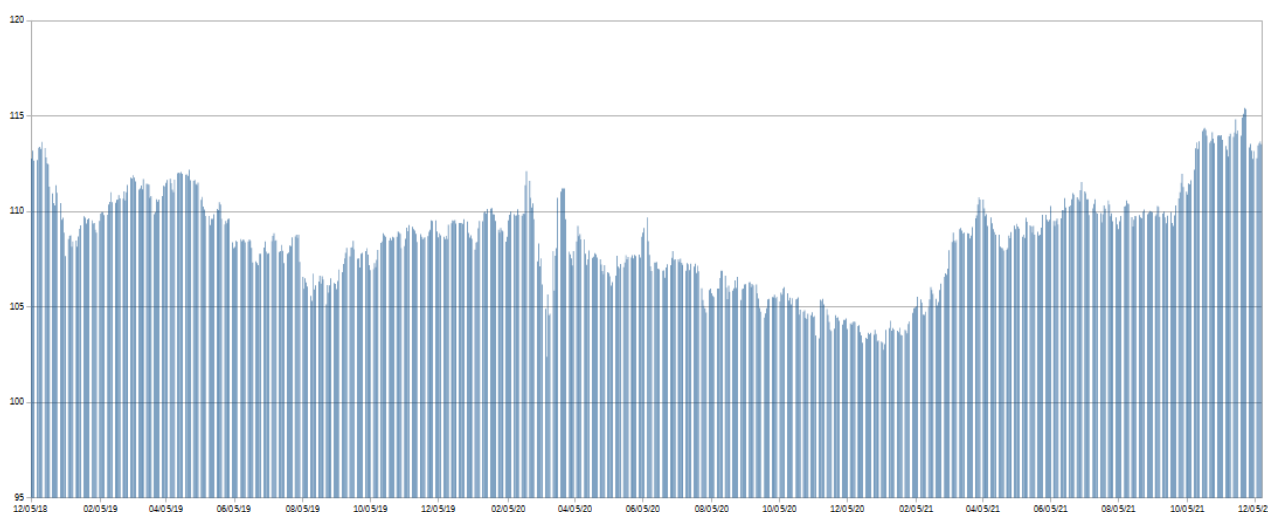


Figure 16. Μεταβολή της JPY/USD ισοτιμίας στο βάθος τους χρόνου



Για την κατασκευή του μοντέλου αρχικά συμπίεστηκαν τα παραπάνω δεδομένα, λαμβάνοντας τον μέσο όρο από κάθε 8 σημεία, στο παραπάνω διάγραμμα. Μετά από αυτή τη διαδικασία, το διάγραμμα μοιάζει κάπως έτσι:

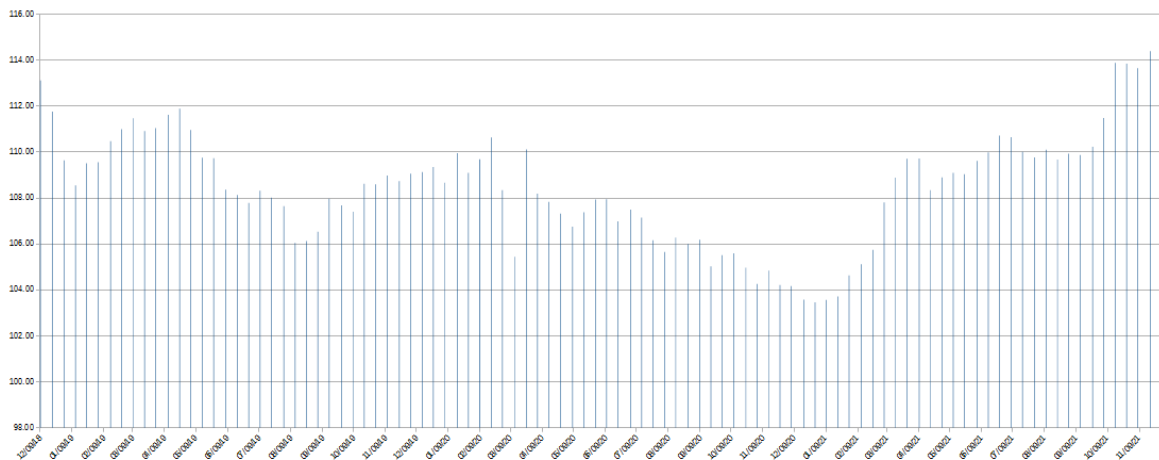


Figure 17. Συμπίεσμένο διάγραμμα της μεταβολής της ισοτιμίας JPY/USD στο βάθος του χρόνου

Όπως φαίνεται το παραπάνω διάγραμμα διατηρεί τη βασική πληροφορία και τα μοτίβα από το πρώτο διάγραμμα και βοηθάει στην εισαγωγή των δεδομένων στο blockchain, σε λογικά χρονικά διαστήματα.

Για την δημιουργία του παραπάνω μοντέλου υλοποιήθηκε στη συνέχεια ένας αλγόριθμος με τη γλώσσα προγραμματισμού Python, για τον υπολογισμό του κατάλληλου όγκου των συναλλαγών, όπου ακολουθούν τα παραπάνω δεδομένα. Το πρόγραμμα, λαμβάνοντας υπόψη το τρόπο λειτουργίας ενός απλού AMM, υπολογίζει μέσω δυναδικής αναζήτησης τον ζητούμενο όγκο των δεδομένων, ο οποίος σε ένα απλό AMM θα οδηγούσε στην ίδια μεταβολή της ισοτιμίας με αυτήν του πραγματικού κόσμου. Στο επόμενο διάγραμμα, με κόκκινο χρώμα, φαίνεται η απόκλιση του μοντέλου που χρησιμοποιήθηκε σε σχέση με το συμπίεσμένο μοντέλο του πραγματικού κόσμου:

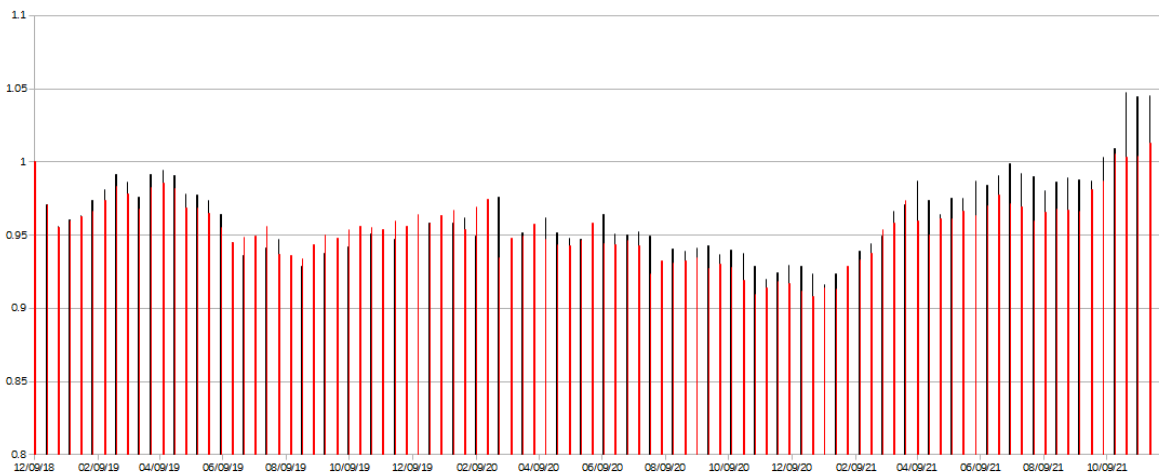


Figure 18. Απόκλιση του JPY/USD μοντέλου σε σχέση με τα δεδομένα του πραγματικού κόσμου

Όπως φαίνεται, το μοντέλο μας είναι αρκετά κοντά με το μοντέλο του πραγματικού κόσμου. Οι αποκλίσεις οφείλονται κυρίως στην έλλειψη ακρίβειας στους αριθμούς υποδιαστολής, επειδή το blockchain εσωτερικά χρησιμοποιεί μόνο ακέραιους αριθμούς και όχι πραγματικούς. Σε ένα πραγματικό AMM, οι περισσότερες αποκλίσεις λύνονται μέσω της προσθήκης ενός επιπλέον φόρου για κάθε συναλλαγή, ο οποίος καλύπτει την ατέλεια της AMM εξίσωσης και των υπολογισμών κι επίσης παρέχει επιπλέον μια ανταμοιβή στο AMM.

Για να δειχθεί καλύτερα η μέθοδος εξισορρόπησης της τιμής και η επαναφορά της ισοτιμίας, η απόκλιση  $\epsilon$  που χρησιμοποιήθηκε μειώθηκε στο 1%, το οποίο σημαίνει ότι η ισοτιμία βρίσκεται κυρίως μεταξύ του εύρους 0.99- 1.01. Το αρχικό μέγεθος από το θησαυροφυλάκιο ορίστηκε ως 5% της συνολικής ρευστότητας. Σε πολλές χώρες στις οποίες γίνεται χρήση μιας τράπεζας αποθεμάτων, το πραγματικό μέγεθος είναι περίπου 10%.

Στο επόμενο διάγραμμα, με μπλε χρώμα, φαίνεται η μεταβολή της ισοτιμίας σε ένα απλό AMM από τις συναλλαγές που ακολουθούν το JPY/USD μοντέλο και με κόκκινο χρώμα, η μεταβολή της ισοτιμίας, όταν οι ίδιες συναλλαγές πραγματοποιούνται στο AMM του DMT πρωτοκόλλου:

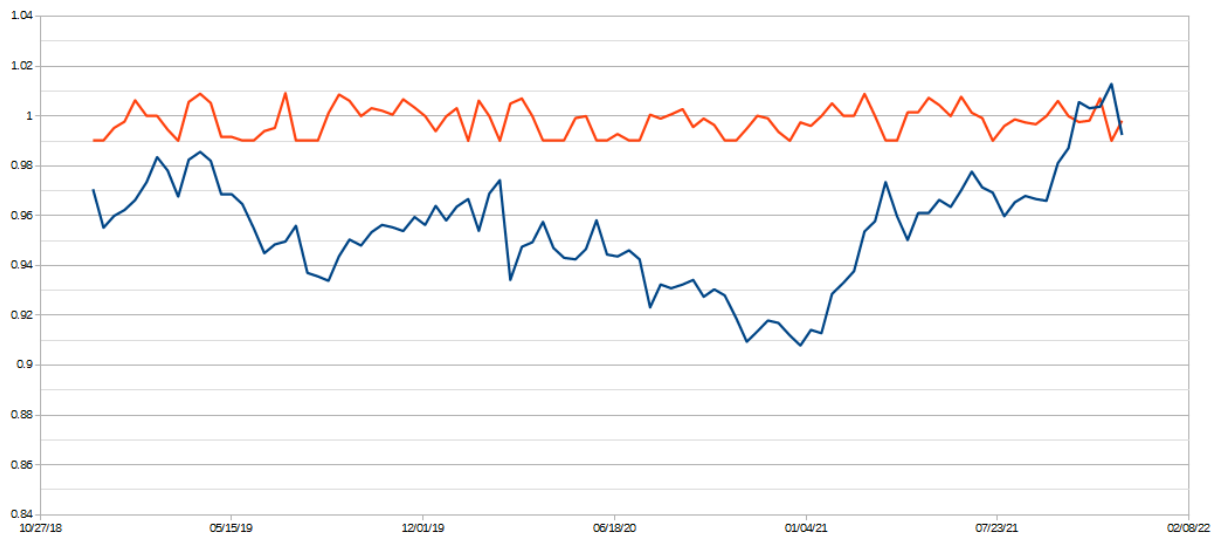


Figure 19. Σύγκριση της μεταβολής της ισοτιμίας σε ένα απλό AMM (μπλε) σε σχέση με το DMT AMM (κόκκινο) από συναλλαγές που ακολουθούν το JPY/USD μοντέλο

Η ισοτιμία στο DMT AMM παρατηρείται ότι διατηρείται σε γενικές γραμμές αρκετά σταθερή, παρά τις έντονες και απρόβλεπτες διακυμάνσεις του JPY/USD μοντέλου.

Έπειτα, δημιουργήθηκε με παρόμοια μεθοδολογία ένα νέο μοντέλο, το οποίο αντικατοπτρίζει πραγματικά δεδομένα από τη μετοχή SAVA (Cassava Sciences, Inc. Common Stock). Οι μεταβολές στην ισοτιμία της μετοχής αυτής φαίνονται στο παρακάτω διάγραμμα:



Figure 20. Μεταβολές στην ισοτιμία της μετοχής SAVA από το Μάρτιο του 2021 μέχρι το Δεκέμβριο του 2021

Όπως παρατηρείται από το παραπάνω διάγραμμα, η μετοχή αυτή παρουσιάζει αρκετά πιο έντονες και απρόβλεπτες διακυμάνσεις στην τιμή της, σε βάθος χρόνου. Σε αυτή την περίπτωση, δεν χρειάστηκε να συμπιεστούν τα αρχικά δεδομένα, καθώς ο αριθμός τους είναι ήδη στα επιθυμητά επίπεδα. Με βάση τον ίδιο αλγόριθμο όπως και προηγουμένως, υπολογίστηκε το μοντέλο των συναλλαγών, οι οποίες μας δίνουν παρόμοιες μεταβολές με αυτές του παραπάνω διαγράμματος, όταν χρησιμοποιούνται σε ένα απλό AMM.

Το παρακάτω διάγραμμα δείχνει και πάλι, με κόκκινο χρώμα, την απόκλιση του μοντέλου μας σε σχέση με τα αρχικά δεδομένα:

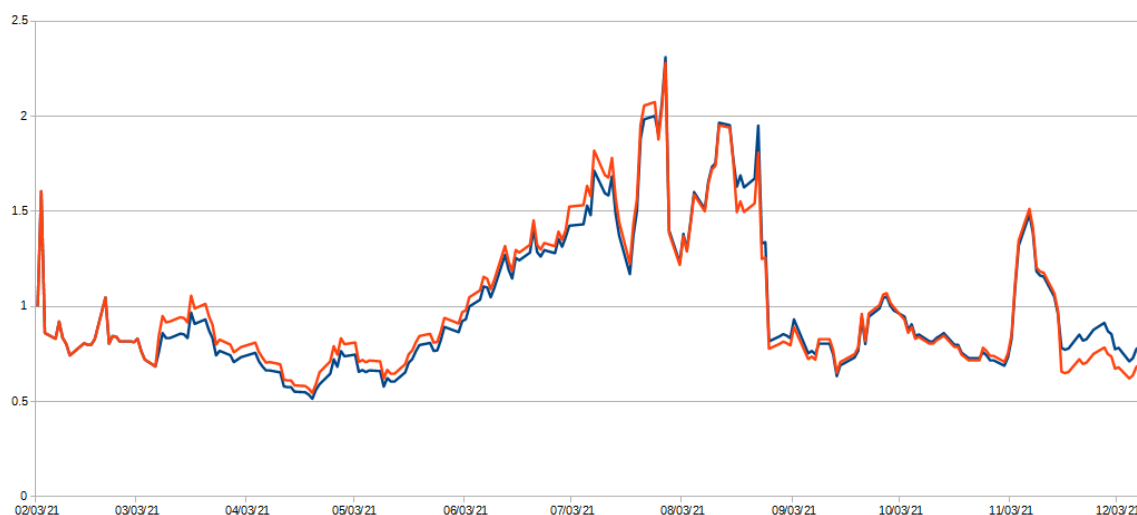


Figure 21. Απόκλιση του SAVA/USD μοντέλου σε σχέση με τα δεδομένα του πραγματικού κόσμου

Επίσης, λόγω ύπαρξης ισχυρών διακυμάνσεων αποφασίστηκε η αύξηση της απόκλισης στο 5%. Τέλος, στο επόμενο διάγραμμα, με μπλε χρώμα, φαίνεται η μεταβολή της ισοτιμίας σε ένα απλό AMM από τις συναλλαγές που ακολουθούν το SAVA/USD μοντέλο και με κόκκινο

χρώμα, η μεταβολή της ισοτιμίας όταν οι ίδιες συναλλαγές του μοντέλου αυτού πραγματοποιούνται στο AMM του DMT πρωτοκόλλου:

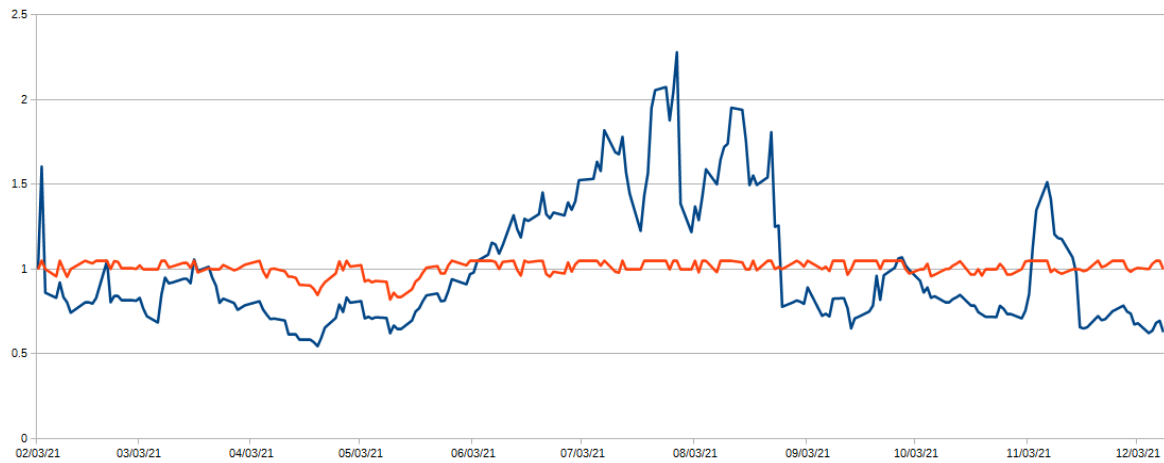


Figure 22. Σύγκριση της μεταβολής της ισοτιμίας σε ένα απλό AMM (μπλε) σε σχέση με το DMT AMM (κόκκινο) από συναλλαγές που ακολουθούν το SAVA/USD μοντέλο

Όπως φαίνεται, το πρωτόκολλο του DMT και σε αυτή την περίπτωση καταφέρνει να διατηρήσει σταθερότητα στην ισοτιμία του, παρά τις πολύ έντονες διακυμάνσεις του αρχικού μοντέλου.

Από τους παραπάνω ελέγχους λοιπόν, επιβεβαιώθηκε ότι το πρωτόκολλο του DMT συμπεριφέρεται σύμφωνα με τις προδιαγραφές του, σε όλα τα στάδια του αλγορίθμου και ακόμη ότι καταφέρνει να διατηρεί σταθερότητα στην ισοτιμία του, ακόμη και όταν έρχεται αντιμέτωπο με μοντέλα του πραγματικού κόσμου, όπως αυτά των κρατικών νομισμάτων ή του χρηματιστηρίου. Στις επόμενες ενότητες, θα περιγραφεί η λειτουργία κάποιων υπαρκτών σταθερών κρυπτονομισμάτων και ο τρόπος που αυτά υλοποιούν την σταθερότητα στις τιμές τους ενώ στο τέλος, θα παρουσιαστούν κάποιες από τις μελλοντικές δυνατότητες των σταθερών κρυπτονομισμάτων.

## 5. Συμπεράσματα & μελλοντική εργασία

Σύμφωνα με τις παρατηρήσεις, η σταθεροποίηση της τιμής ενός κρυπτονομίσματος, όπως είναι το DMT, στην τιμή ενός άλλου νομίσματος, όπως π.χ. είναι το δολάριο, βασίζεται στη χρήση κάποιων κοινών πρακτικών με αυτών της Ομοσπονδιακής Τράπεζας Αποθεμάτων [49]. Οι πιο συνήθεις από αυτές τις ενέργειες, είναι η μεταβολή της συνολικής προσφοράς, όπως στην περίπτωση του DMT ή η μεταβολή των επιτοκίων, όπως στην περίπτωση του MakerDAO. Τι θα γίνει αν όμως ένα σταθερό κρυπτονόμισμα, σε βάθος χρόνου, αναπτυχθεί στο σημείο που να έχει τόσους χρήστες, όπως το δολάριο ή οποιοδήποτε άλλο εθνικό νόμισμα; Αν συνέβαινε κάτι τέτοιο, αυτό το σταθερό κρυπτονόμισμα θα προσέφερε για πρώτη φορά πλήρη διαφάνεια, αποκεντροποίηση και αλγοριθμική σταθερότητα παγκοσμίως. Κάτι τέτοιο δεν μπορεί να αναπτυχθεί με οποιαδήποτε νομισματική πολιτική. Ας δούμε τί σημαίνει αυτό για το μέλλον των σταθερών κρυπτονομισμάτων.

### 5.1. Σταθεροποίηση στο Δείκτη Τιμών του Καταναλωτή

Σε ένα μελλοντικό κόσμο, στον οποίο ένα μεγάλο ποσοστό των συναλλαγών που γίνονται, πραγματοποιούνται μέσω ενός σταθερού κρυπτονομίσματος, το οποίο ονομάζεται για ευκολία “Stable”, θα σημαίνει ότι και πολλά αγαθά ή υπηρεσίες θα πωλούνται με βάση την τιμή του Stable. Σε έναν τέτοιο κόσμο, η τιμή του Stable θα μπορούσε να καρφωθεί σε έναν δείκτη αντί για κάποιο άλλο κρατικό νόμισμα, όπως για παράδειγμα είναι ο δείκτης τιμών του καταναλωτή. Κάτι τέτοιο είναι παρόμοιο με τον τρόπο με τον οποίο η Ομοσπονδιακή Τράπεζα σταθεροποιεί τη τιμή του δολαρίου, σύμφωνα με τον δείκτη τιμών του καταναλωτή (CPI), ώστε να διατηρεί σταθερή την αγοραστική δύναμη του δολαρίου. Αν επίσης αποδειχθεί ότι η προσθήκη ενός τεχνητού ετήσιου πληθωρισμού παράγει καλύτερα αποτελέσματα, το πρωτόκολλο του Stable θα μπορούσε να συμπεριλάβει έναν τεχνητό πληθωρισμό στους υπολογισμούς του, παρομοιάζοντας ακόμη περισσότερο τις λειτουργίες της Κεντρικής Τράπεζας.

Θα μπορούσε κάποιος να φανταστεί πληθώρα πλεονεκτημάτων από αυτήν την μέθοδο. Αρχικά, σε αντίθεση με την Κεντρική Τράπεζα, το Stable υλοποιεί την νομισματική του πολιτική μέσω ενός πλήρως αποκεντρωμένου και διαφανούς αλγορίθμου, χωρίς να χρειάζεται ανθρώπινη παρέμβαση. Αν και μια πλήρως αυτοματοποιημένη νομισματική πολιτική έχει τους κινδύνους της, θεωρείται ότι η υιοθέτηση και η χρήση ενός σταθερού κρυπτονομίσματος, θα παρακινήσει με τη σειρά της επιπλέον έρευνα σε αλγοριθμικές νομισματικές πολιτικές.

Ακόμη, αν η τιμή του Stable είναι καρφωμένη στην τιμή του δείκτη τιμών του καταναλωτή, αυτό σημαίνει ότι το πρωτόκολλο και η αντίστοιχη νομισματική του πολιτική είναι ανεξάρτητα από οποιαδήποτε κυβέρνηση. Σε γενικές γραμμές, οι κυβερνήσεις προσφέρουν κυρίως δυο λειτουργίες προκειμένου να εξασφαλίσουν έλεγχο πάνω στην τρέχουσα προσφορά χρήματος: Προστασία από την πλαστογραφία και σταθερότητα των τιμών. Όσον αφορά στην σταθερότητα των τιμών, μια κεντρική τράπεζα βοηθάει στην εξομάλυνση της μακροοικονομικής ζήτησης και σε κάποιες περιπτώσεις, στη διαχείριση της ανεργίας. Η ανάπτυξη του Bitcoin και των υπόλοιπων κρυπτονομισμάτων εξάλειψε την ανάγκη για μια

κεντρική αρχή, η οποία επαληθεύει την εγκυρότητα των νομισμάτων, καθώς πλέον αυτό πραγματοποιείται μέσω του blockchain. Επίσης, ένα νόμισμα όπως το Stable, απαλείφει την ανάγκη ύπαρξης μιας κεντρικής αρχής για την διασφάλιση της σταθερότητας των τιμών. Όσο καλές προθέσεις και να έχουν οι κεντρικές τράπεζες, σε κρίσιμες περιόδους, οι κυβερνήσεις θα προσπαθήσουν να τυπώσουν νέο χρήμα, ώστε να γλιτώσουν το δημοσιονομικό χρέος. Αν μια τέτοια τεχνολογία υιοθετηθεί από τους πολίτες μιας κοινωνίας, θα προσφέρει, για πρώτη φορά, μια καινοτόμα μορφή χρηματοοικονομικής διαφάνειας και λογοδοσίας, η οποία δεν ήταν μέχρι τώρα δυνατή.

Τέλος, κάποιοι μπορεί να ισχυριστούν ότι αν το Stable καρφωνόταν στον δείκτη τιμών καταναλωτή, τότε θα εξυπηρετούσε μόνο μια από τις δύο λειτουργίες της κεντρικής τράπεζας. Πιο συγκεκριμένα, ενώ το πρωτόκολλο θα βοηθούσε στη διατήρηση της σταθερότητας των τιμών, θα αγνοούσε εντελώς το πρόβλημα της ανεργίας. Αυτή η ανεπάρκεια του όμως, μπορεί να διορθωθεί. Ας σκεφτούμε τον τρόπο με τον οποίο η Ομοσπονδιακή Αρχή βοηθάει στην σταθεροποίηση των επιπέδων ανεργίας. Σε περιόδους κατά τις οποίες η οικονομία βρίσκεται σε πλήγμα, οι επιχειρήσεις αρχίζουν να προσφέρουν χαμηλότερους μισθούς και λιγότερες θέσεις εργασίας, αυξάνοντας τα επίπεδα ανεργίας. Παρατηρώντας το αυτό, η κεντρική τράπεζα εκτυπώνει καινούργια χρήματα και τα διανέμει στην οικονομία, με την προοπτική ότι έτσι θα επανέλθουν οι τιμές και θα επανέλθει η ανεργία στα αρχικά της επίπεδα. Το πρωτόκολλο του Stable όμως, μπορεί επίσης να υλοποιήσει έναν παρόμοιο επιπλέον μηχανισμό στο πρωτόκολλο του, δημιουργώντας και διανέμοντας νέα νομίσματα, σε περιόδους υψηλής ανεργίας, ακριβώς όπως και η κεντρική τράπεζα. Αυτό που χρειάζεται είναι να προστεθεί μια επιπλέον παράμετρος στο πρωτόκολλο, η οποία να μετράει τα επίπεδα ανεργίας ή της συνολικής ανάπτυξης, την συγκεκριμένη χρονική στιγμή. Με αυτό τον τρόπο, το πρωτόκολλο του Stable μπορεί να μιμηθεί τις λειτουργίες της κεντρικής τράπεζας, παραμένοντας ταυτόχρονα πλήρως διαφανές και αλγοριθμικά αποκεντροποιημένο.

## **5.2. Ένα τοπικό Stable νόμισμα για κάθε χώρα**

Αν και η ιδέα ενός μοναδικού παγκόσμιου νομίσματος μπορεί να φαίνεται ελκυστική, στην πραγματικότητα είναι καλύτερο κάθε κοινωνία να έχει το δικό της νόμισμα, ώστε να μπορεί να αντιδράσει με βάση τις τοπικές μεταβολές στη ζήτηση. Πολλές φορές, μπορεί να προκύψουν αναταραχές στη ζήτηση, οι οποίες παρατηρούνται σε ένα τοπικό εύρος κι όχι παγκόσμια. Κάτι τέτοιο είναι εμφανές τον τελευταίο καιρό στην Ευρωζώνη, όπου η Ελλάδα αντιμετωπίζει ένα ισχυρό πλήγμα στη ζήτησή της, ενώ η υπόλοιπη κεντρική Ευρώπη, όπως η Γερμανία, παρουσιάζει κανονικά επίπεδα ζήτησης. Αν σε μια τέτοια περίπτωση η Ελλάδα και η Γερμανία χρησιμοποιούν το ίδιο νόμισμα, τότε δεν μπορεί να εφαρμοστεί κάποιο είδους επεκτατικής νομισματικής πολιτικής ώστε να επανέλθει η ζήτηση στην οικονομία της Ελλάδας και λόγω αυτού, αντιμετωπίζει προβλήματα από αυτή την σταθερότητα της προσφοράς. Για αυτό τον λόγο, είναι ωφέλιμο κάθε οικονομία να υλοποιήσει το δικό της σταθερό κρυπτονόμισμα και να το σταθεροποιήσει στον δείκτη τιμών καταναλωτή της χώρας. Έτσι, η οικονομία κάθε χώρας θα λειτουργεί, όπως σήμερα, με την επιπλέον προσθήκη της διαφάνειας και της αποκεντροποίησης που παρέχει το blockchain [50].

## Βιβλιογραφία

- [1] Lamport L., Shostak R., Pease M., “The Byzantine Generals Problem”, <https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf>, 1982 [2] Lamport L., Shostak R., Pease M., “The Byzantine Generals Problem”, <https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf>, 1982
- [2] Wadsworth A., ““Decrypting the role of distributed ledger technology in payments processes”, <https://www.rbnz.govt.nz/-/media/reservebank/files/publications/bulletins/2018/2018may81-05.pdf>, 2018.
- [3] Nakamoto S., “Bitcoin: A peer-to-peer electronic cash system”, [https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging\\_Tech\\_Bitcoin\\_Crypto.pdf](https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf), 2008.
- [4] Daily Bit, “9 Types of Consensus Mechanisms That You Didn’t Know About”, <https://medium.com/the-daily-bit/9-types-of-consensus-mechanisms-that-you-didnt-know-about-49ec365179da>, 2018.
- [5] Buterin, V., “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”, 2014.
- [6] Hollander L., “The Ethereum Virtual Machine – How does it work?”, <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e>, 2019.
- [7] Reiff N., “Decentralized Autonomous Organization (DAO)”, <https://www.investopedia.com/tech/what-dao/>, 2021.
- [8] Fatas A., Weder di Mauro B., “The benefits of a global digital currency”, <https://voxeu.org/article/benefits-global-digital-currency>, 2019
- [9] Buterin V., “The Meaning of Decentralization”, <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>, 2017
- [10] Frowis M., Bohme R., ““In code we trust? Measuring the control flow immutability of all smart contracts deployed on Ethereum”, <https://www.semanticscholar.org/paper/In-Code-We-Trust-Measuring-the-Control-Flow-of-All-Fr%C3%B6wis-B%C3%B6hme/9e50e037471aeac481c2c97f0ae8c9ee1ff64acf>, 2019.
- [11] Bullmann D., Klemm J., Pinna A., “In search for stability in crypto-assets: are stablecoins the solution?”, <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf>, 2019.
- [12] Sams. R., “A Note on Cryptocurrency Stabilisation: Seigniorage Shares”, <https://blog.bitmex.com/wp-content/uploads/2018/06/A-Note-on-Cryptocurrency-Stabilisation-Seigniorage-Shares.pdf>, 2014.

- [13] “The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System”, <https://makerdao.com/en/whitepaper#abstract>, 2014.
- [14] Manrique S., “What is DAI, and how does it work?”, <https://medium.com/mycrypto/what-is-dai-and-how-does-it-work-742d09ba25d6>, 2019.
- [15] “Tether: Fiat currencies on the Bitcoin blockchain”, <https://whitepaper.io/document/6/tether-whitepaper>.
- [16] White L. H., “The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold”, <https://www.cato.org/sites/cato.org/files/serials/files/cato-journal/2014/5/cato-journal-v34n2-5.pdf>, 2014.
- [17] Vigna P., Russolillo S., “The Mystery Behind Tether, the Crypto World’s Digital Dollar”, <https://www.wsj.com/articles/the-mystery-behind-tether-the-crypto-worlds-digital-dollar-1534089601>, 2018.
- [18] Griffin J. M., Shams A., “Is Bitcoin Really Untethered?”, <https://onlinelibrary.wiley.com/doi/full/10.1111/jofi.12903>, 2020.
- [19] Centre, “USDC Whitepaper”, <https://whitepaper.io/document/716/usd-coin-whitepaper>, 2018.
- [20] “BUSD Whitepaper”, <https://www.allcryptowhitepapers.com/binance-usd-whitepaper/>.
- [21] Larimer D, Hokinson C., Larimer S., “BitShares A Peer-to-Peer Polymorphic Digital Asset Exchange”.
- [22] Kuo E., Iles B., Rincon-Cruz M., “Ampleforth: A New Synthetic Commodity”, <https://www.ampleforth.org/papers/>, 2019.
- [23] “Dollarization: Theoretical and Empirical Models”, <http://web.worldbank.org/archive/website00960A/WEB/OTHER/84E2905B.HTM> .
- [24] Mecagni M., Maino R., “Dollarization in Sub-Saharan Africa: Experience and Lessons”, <https://www.imf.org/external/pubs/ft/dp/2015/afr1504.pdf>, 2015.
- [25] Hager N., “Blue Dollar, Black Market: The Illegal Exchange Rate as a Financial Indicator in Argentina”, <https://www.coha.org/blue-dollar-black-market-the-illegal-exchange-rate-as-a-financial-indicator-in-argentina/>, 2014.
- [26] Hazlett P. K., Luther W. J., “Is bitcoin money? And what that means”, <https://www.sciencedirect.com/science/article/abs/pii/S1062976919301528>, 2020. [27] Larimer D, Hokinson C., Larimer S., “BitShares A Peer-to-Peer Polymorphic Digital Asset Exchange”.
- [27] Ragnedda M., Destefanis G., “Blockchain and web 3.0: Social, Economic and Technological Challenges.”, <https://www.taylorfrancis.com/books/edit/10.4324/9780429029530/blockchain-web-3-0-massimo-ragnedda-giuseppe-destefanis>, 2020.



- [28] Petralia K., Philippon T., Rice T., Veron N., “Banking Disrupted? Financial Intermediation in an Era of Transformational Technology”, <https://voxeu.org/content/banking-disrupted-financial-intermediation-era-transformational-technology>, 2019.
- [29] McLaughlin T., “Two Paths to Tomorrow’s Money”, <https://www.citibank.com/icg/bcma/psg/assets/docs/Tomorrow-Money-Citi.pdf>, 2020.
- [30] Murphy A., “An Analysis of the Financial Crisis of 2008: Causes and Solutions”, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1295344](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1295344), 2008.
- [31] “Deflationary Spiral”, [https://en.bitcoin.it/wiki/Deflationary\\_spiral](https://en.bitcoin.it/wiki/Deflationary_spiral).
- [32] Lyons R. K., Viswanath-Natraj G., ““What Keeps Stablecoins Stable?””, [https://www.nber.org/system/files/working\\_papers/w27136/w27136.pdf](https://www.nber.org/system/files/working_papers/w27136/w27136.pdf), 2020.
- [33] Black F (2012), “Business Cycles and Equilibrium”.
- [34] Friedman M. (1989) Quantity Theory of Money. In: Eatwell J., Milgate M., Newman P. (eds) Money. The New Palgrave. Palgrave Macmillan, London, [https://doi.org/10.1007/978-1-349-19804-7\\_1](https://doi.org/10.1007/978-1-349-19804-7_1).
- [35] “OpenZeppelin Documentation”, <https://docs.openzeppelin.com/>.
- [36] “Non-fungible tokens (NFT)”, <https://ethereum.org/en/nft/>.
- [37] “EIP-721: Non-Fungible Token Standard”, <https://eips.ethereum.org/EIPS/eip-721>, 2018.
- [38] “Opensea Marketplace”, <https://opensea.io/>.
- [39] “LooksRare Marketplace” <https://looksrare.org/>.
- [40] Martinelli F., “What is an Automated Market Maker (AMM)?”, <https://medium.com/balancer-protocol/what-is-an-automated-market-maker-amm-588954fc5ff7>, 2021.
- [41] Onyschenko S., “AMM Types & Differentiations”, <https://blaize.tech/article-type/amm-types-differentiations/>, 2020.
- [42] Erins P., “How to calculate Impermanent Loss: full derivation”, <https://medium.com/auditless/how-to-calculate-impermanent-loss-full-derivation-803e8b2497b7>, 2021.
- [43] “Arbitrage”, Investopedia, <https://www.investopedia.com/terms/a/arbitrage.asp>.
- [44] Atzori M., “Blockchain Technology and Decentralized Governance: Is the State Still Necessary?”, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2709713](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713), 2016.
- [45] “Solidity Documentation”, <https://docs.soliditylang.org/en/develop/>.
- [46] Antonopoulos A., Wood G., “Mastering Ethereum”, <https://github.com/ethereumbook/ethereumbook>.
- [47] “Truffle Documentation”, <https://trufflesuite.com/docs/index.html>.

- [48] “An Introduction to Binance Smart Chain (BSC)”,  
<https://academy.binance.com/en/articles/an-introduction-to-binance-smart-chain-bsc>.
- [49] European Central Bank (2020), “Stablecoins – no coins, but are they stable?”,  
<https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191128.en.pdf>.
- [50] Constancio V., “The future of monetary policy frameworks”,  
<https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170525.en.html>, 2018.