zelcash

καινοτόμο | διαισθητικό | ευφυές

Λευκή Βίβλος Έκδοση 2

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Εισαγωγή

Η τεχνολογία Blockchain θα αλλάξει τον κόσμο με τρόπους που δεν θα μπορούσαμε να έχουμε φανταστεί πριν πέντε χρόνια. Η "MarketsandMarkets" προβλέπει μία ετήσια αύξηση της τάξεως του 61.5% τουλάχιστον έως το έτος 2021, και η έκθεση του Παγκόσμιου Οικονομικού Φόρουμ προβλέπει ότι μέχρι το 2027 το 10% του Ακαθάριστου Παγκόσμιου Προϊόντος (GDP) θα βρίσκεται αποθηκευμένο σε τεχνολογία blockchain. [1],[2]

Η διαφάνεια, σταθερότητα και η αμεσότητα της τεχνολογίας blockchain, καταργεί την ανάγκη του μεσάζοντα μειώνοντας τις προμήθειες, ενισχύει την ασφάλεια, και εξαλείφει τον κίνδυνο καταβολής αποζημιώσεων. Παρέχει απλότητα: Οι διαδικασίες προστίθενται σε ένα ενιαίο δημόσιο κατάστιχο (ledger), αποφεύγοντας την ακαταστασία το χάος και τους πονοκεφάλους που γενικώς σχετίζονται με τα πολλαπλά κατάστιχα (multiple ledgers).

Ίσως ο σημαντικότερο, η τεχνολογία blockchain ισχυροποιεί τους ανθρώπους, δίνοντας τους περισσότερο έλεγχο επί των συναλλαγών τους και την δυνατότητα της αλληλεπίδρασης με τις πληροφορίες των οικονομικών συναλλαγών που παρέχονται (προστασία προσωπικών δεδομένων).

Είναι ξεκάθαρο ότι η τεχνολογία blockchain παρέχει τεράστια δυνατότητα αναμόρφωσης της ιδιωτικότητας και της ασφάλειας και υπό ιδανικές συνθήκες να καταφέρει να αναδιαμορφώσει την παγκόσμια οικονομία.

Αλλά *μόνο* ιδανικά, έως αυτό το σημείο. Η έλλειψη δυνατότητας πρόσβασης και χρηστικότητας έχουν καθυστερήσει την μαζική υιοθέτηση. Τα θέματα ευελιξίας (scalability) βρίσκονται σε αφθονία. Άλλες προκλήσεις περιλαμβάνουν Επιθέσεις Διανεμημένης Άρνησης Εξυπηρέτησης (DDoS) η κατάρρευση ανταλλακτηρίων η έλλειψη διόδων διακίνησης του κοινού χρήματος (FIAT) και ειδικά για το μέσο χρήστη -- ένα δυσκολονόητο σύστημα δεκαεξαδικών διευθύνσεων. Το αποτέλεσμα: απομονωμένα οικοσυστήματα, ευπάθειες ασφάλειας, και υψηλά -- μερικές φορές αξεπέραστα -- εμπόδια εισόδου.

Όπως περιγράφεται σε αυτή την εργασία, σκοπεύουμε να αντιμετωπίσουμε -- ακόμη και λύσουμε -- αυτά τα ζητήματα.

Η πλατφόρμα μας παρέχει μια διαισθητική, ανεμπόδιστη εμπειρία, διευκολύνοντας τις συναλλαγές "cross-chain" με ένα απλό και καθαρό περιβάλλον εργασίας για τους απλούς χρήστες καθώς και για τους προγραμματιστές. Με το Zel, δημιουργήσαμε ένα "όλα σε ένα" τυποποιημένο περιβάλλον που επιτρέπει σε προγραμματιστές να επικεντρώσουν την προσπάθεια τους στην εξεύρεση λύσεων τεχνολογίας blockchain. Αυτό θα ενθαρρύνει την ελεύθερη δημιουργία των Αποκεντρωμένων Εφαρμογών

(DApps) και έξυπνων συμβολαίων που είναι ανοιχτά προς όλους.

Το όραμα που μνημονεύεται και οι λύσεις που περιγράφονται σε αυτή τη "λευκή βίβλο" (whitepaper) αντιπροσωπεύουν τα πρώτα βήματα προς την κατάργηση των εμποδίων που προαναφέρθηκαν, οδηγώντας στην παγκόσμια υιοθέτηση της τεχνολογίας blockchain και της αποτελεσματικής διατάραξης του παγκόσμιου οικονομικού γίγνεσθαι.

---

[1] "Blockchain Technology Market--Global Forecast to 2021" MarketsandMarkets research *Blockchain Daily News*
[2] Deep Shift Technology Tipping Points and Societal Impact --World Economic Forum
www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Αποστολή, Όραμα και Αξίες

Η ομάδα του Zelcash ιδρύθηκε από ομοϊδεάτες που πιστεύουν ότι η τεχνολογία μπορεί να προσφέρει τα μέγιστα στην εξέλιξη της ανθρωπότητας. Πιστεύουμε στο όραμα ενός αποκεντρωμένου κόσμου, όπου θα βελτιωθούν τα πάντα. Έχουμε θέσει έναν στόχο ως ομάδα, να γίνουμε **οι μπροστάρηδες στην ανάπτυξη της τεχνολογίας blockchain και της προστασίας της ιδιωτικότητας.** Η κοινότητά μας θα είναι η κινητήριος δύναμη του προγράμματος, λαμβάνοντας έμπνευση από άλλους του ίδιου χώρου. Ο στόχος μας είναι να γίνουμε ηγέτες της βιομηχανίας blockchain αφήνοντας την ίδια την τεχνολογία να τραβήξει το πρόγραμμα δια μέσω της ενασχόλησης της κοινότητας. Το Zelcash σκοπεύει να δημιουργήσει τα απαραίτητα εργαλεία ώστε να καταστεί εφικτό στους προγραμματιστές να διευρύνουν τις εντυπωσιακές δυνατότητες της τεχνολογίας blockchain, οδηγούμενη από την ισχυρή μας ομάδα και την στιβαρή μας κοινότητα ώστε να διαθέσουμε ισχυρή τεχνολογία προσβάσιμη για όλους.

Το Zel στην κορύφωση του αποσκοπεί στο να έχει γίνει ένα πλήρως αποκεντρωμένο και κλιμακούμενο παγκόσμιο δίκτυο υπολογιστικής ισχύος το οποίο θα επιτρέπει στους προγραμματιστές να αξιοποιήσουν την πλήρη δύναμη του διαδικτύου χωρίς δεσμεύσεις, παροχή εύκολων στην χρήση οικονομικών συναλλαγών σε μη προνομιούχους ανθρώπους που ζουν σε χώρες χωρίς πρόσβαση στο παραδοσιακό τραπεζικό σύστημα, και επέκταση των φαινομενικά απεριόριστων δυνατοτήτων της τεχνολογίας blockchain.

Επισκόπηση

Σκοπός αυτής της εργασίας είναι η παροχή εις βάθος ανάλυσης των τεχνολογιών Zel και των χαρακτηριστικών γνωρισμάτων που έχουν κυκλοφορήσει ή αναμένεται η κυκλοφορία τους. Θέλουμε αυτή η εργασία να είναι κατανοητή και προσβάσιμη στους πάντες, ενώ σύγχρονος θα διασφαλίσουμε ότι οι τεχνολογίες κλειδί θα συζητηθούν. Δεν θα παρασχεθούν εις βάθος τεχνικές λεπτομέρειες για ακυκλοφόρητα προϊόντα έως ότου οι Τεχνολογίες Zel τα κυκλοφορήσουν, ή λίγο πριν την κυκλοφορία τους, σε δημόσια χρήση. Αυτό θα εξασφαλίσει ότι η ανάπτυξη του προϊόντος Τεχνολογιών Zel δεν θα αντιγραφεί προ της κυκλοφορίας του.

Παρότι κάποια από τα προϊόντα του Zel είναι "κλειστού κώδικα" (όπως είναι το Zeltrez) , ο κώδικας τους θα ελεγχθεί από ένα ανεξάρτητο τρίτο μέρος. Η ομάδα του Zel πιστεύει στο "ελεύθερο λογισμικό", και όπου είναι εφικτό, θα διασφαλίσουμε ότι το λογισμικό μας και οι τεχνολογίες που θα κυκλοφορήσουν θα είναι ανοιχτού κώδικα, καθώς και οι τεχνικές τους λεπτομέρειες.

Ως εκ τούτου, αυτή η λευκή βίβλος δεν προορίζεται ως τεχνικό εγχειρίδιο η φυλλάδιο οδηγιών, αλλά ως ένα μέσο που αποκαλύπτει το τι έχουμε επιτύχει έως τώρα καθώς και στο να γνωστοποιήσει το όραμα μας και τα σχεδία μας καθώς εργαζόμαστε προς την υλοποίηση των πραγματικών δυνατοτήτων του Zel. Σε αυτό το πνεύμα λάβετε παρακαλώ υπόψη την παρακάτω αποποίηση ποινικής ευθύνης:

Αποποίηση Ποινικής Ευθύνης: Προνοητικές Δηλώσεις

Οι πληροφορίες σε αυτή την λευκή βίβλο (whitepaper) είναι καθαρά περιγραφικές και όχι δεσμευτικές. Παρακαλώ σημειώστε ότι αυτό το έγγραφο περιλαμβάνει προβλέψεις, δηλώσεις προθέσεων, συζήτηση σχεδίων, εκτιμήσεις και άλλες πληροφορίες που θα μπορούσαν να χαρακτηριστούν προβλέψεις για το μέλλον. Παρότι αυτές οι προβλέψεις απηχούν την προσωπική μας κρίση και προσδοκίες του τι μας επιφυλάσσει το μέλλον, αυτό δεν αποτελεί μια προσφορά ή παράκληση να αγοραστεί οποιοδήποτε προϊόν, υπηρεσία ή ασφάλεια. Όλα τα αναγραφόμενα υπόκεινται σε ρίσκο και αβεβαιότητα σε τέτοιο βαθμό που θα μπορούσε να μπορούσε να έχει ως αποτέλεσμα την σημαντική απόκλιση των πραγματικών αποτελεσμάτων από τα προσδοκώμενα. Καμία πληροφορία που παρέχεται σε αυτή την λευκή βίβλο δεν έχει ελεγχθεί η εγκριθεί από κάποια ρυθμιστική ή εποπτική αρχή.

Επιπλέον, σκοπεύουμε να χρησιμοποιήσουμε την τεχνολογία Zel blockchain ως πλατφόρμα προγραμματισμού ανοιχτού κώδικα, συμβάλλοντας σε αυτές τις τεχνολογίες υπό το καθεστώς της "άδειας ανοιχτού λογισμικού" με σκοπό την ωφέλεια της ανθρωπότητας, και όχι επικεντρώνοντας αποκλειστικά στο οικονομικό κέρδος των

εμπλεκόμενων στο πρόγραμμα. Για τον λόγο αυτό παρακαλούμε να μην επιδείξετε τυφλή εμπιστοσύνη, ειδικά σε ότι αφορά οικονομικές αποφάσεις, σε τέτοιου είδους μελλοντικές προβλέψεις που ανά πάσα στιγμή δύναται να αλλάξουν.

Αυτή η λευκή βίβλος και οι προηγούμενες καθώς και οι μελλοντικές εκδόσεις θα είναι διαθέσιμες στον ιστότοπο: zel.cash/whitepaper. Η πρωτότυπη (μη μεταφρασμένη) έκδοση είναι γραμμένη στην επίσημη Αγγλική. *Σημείωση: Αυτό το κείμενο θα ανανεώνεται συχνά, ορισμένες φορές χωρίς προειδοποίηση. Παρακαλούμε επιβεβαιώστε ότι η έκδοση που διαβάζετε είναι η πιο πρόσφατη.*

1.0 Bitcoin

Ο Ιανουάριος του 2009 σημαδεύτηκε από την κυκλοφορία του Bitcoin από τον Satoshi Nakamoto. Ως το πρώτο νόμισμα χωρίς κεντρική τράπεζα, η εκδότη και χωρίς φυσική υποστήριξη, αντιπροσώπευε μια ριζοσπαστική επανάσταση στον τρόπο λειτουργίας των οικονομικών συστημάτων. Αναμφισβήτητα το πολύ πιο σημαντικό σημείο από την απλή συναλλαγή αγαθών ήταν η τεχνολογία στην οποία βασιζόταν.
Η τεχνολογία blockchain, η οποία επίσης δημιουργήθηκε από τον Nakamoto, επέτρεψε την χρήση της Αποκεντρωμένης και Διανεμημένης Συναίνεσης. Αφαιρώντας τον κεντρικό εκδότη η ελεγκτή, το "ηλεκτρονικό χρήμα" θα επέτρεπε τις συναλλαγές "χρήστη προς χρήστη" (peer to peer), χωρίς την συναίνεση η την επιβεβαίωση από ένα έμπιστο οργανισμό που δρα ως τρίτο μέρος.

Το Bitcoin δεν ήταν το πρώτο ηλεκτρονικό χρήμα. Το b-money του Dei και άλλα προϋπήρχαν του Bitcoin. Το πρόβλημα τους ωστόσο ήταν η επίτευξης της συναίνεσης. Υπήρχε η ανάγκη δημιουργίας ενός μηχανισμού εξουδετέρωσης ενός κακόβουλου χρήστη που θα εξαπέλυε "επίθεση διπλής χρέωσης προς το δίκτυο". Με την χρησιμοποίηση της "απόδειξης παροχής έργου" (POW) για την επιβεβαίωση των blocks στο blockchain του bitcoin (μια παρόμοια μέθοδος με το Hashcash του Adam Back), θα επιτυγχάνονταν συναίνεση μεταξύ των κόμβων, επιτρέποντας την επιβεβαίωση των συναλλαγών.

Η τεχνολογία blockchain έκτοτε εξελίσσεται συνεχώς. Η ανάπτυξη διάφορων πρότζεκτ (με πιο αξιοσημείωτο το Ethereum) έχει δείξει νέες δυνατότητες και χρήσεις για την τεχνολογία blockchain, διευρύνοντας τις δυνατότητες της.

1.5 Zcash

Το Zerocash(2014), το οποίο αργότερα έγινε το Zcash project (2016), χρησιμοποιούσε την τεχνολογία κρυπτογράφησης zk-SNARKs (Zero- knowledge Succinct Non-interactive ARguments of Knowledge) με σκοπό να παράσχει πραγματικά ανώνυμες συναλλαγές κόμβο προς κόμβο. Χτίζοντας πάνω στο Bitcoin το Zcash εξελίχθηκε από το αρχικό Zerocash με διορθώσεις ασφαλείας και προσαρμογές καθώς επίσης και με βελτίωση της λειτουργικότητας και της απόδοσης. Με τον ίδιο τρόπο που το bitcoin έγινε το πρώτο ευρέος αποδεκτό ψηφιακό νόμισμα, το Zcash έγινε το πρώτο ευρέος αποδεκτό ανώνυμο ψηφιακό νόμισμα.

Επίσης το Zcash ξεκίνησε μια μάχη εναντίον της συγκεντρωτικότητας της διαδικασίας "εξόρυξης" που είχε προκληθεί από τους SHA-256 ASICs που είχαν

κυριαρχήσει στο δίκτυο του bitcoin. Μια τέτοια εξέλιξη κατά γενική ομολογία βλάπτει την αποκέντρωση του δικτύου διότι βγάζει τον απλό οικιακό χρήστη από την διαδικασία της "εξόρυξης" του νομίσματος. Η εισαγωγή του "Equihash", ενός απαιτητικού στην μνήμη αλγόριθμου εξόρυξης "απόδειξης παροχής έργου" (POW), επανέφερε την διαδικασία της "εξόρυξης" στο μονοπάτι της αποκέντρωσης με την χρήση επεξεργαστών και καρτών γραφικών υπολογιστή. Παρότι πρόσφατα αναπτύχθηκαν ASICs για το Zcash's Equihash 200.9, άλλα πρότζεκτ καταφέρνουν και παραμένουν αποκεντρωμένα με τις συχνές αλλαγές αλγορίθμων εξόρυξης όπως είναι το τροποποιημένο Equihash και το ProgPOW, καθώς και μέσω νέων επινοήσεων όπως είναι η "απόδειξη παροχής χρήσιμου έργου" (proof of useful work).

Το zk-SNARKs επιτρέπει την εκτέλεση μιας λειτουργίας (όπως μία συναλλαγή που μεταδίδεται στο δίκτυο blockchain) της οποίας ο αποστολέας το ποσό που διακινήθηκε και ο παραλήπτης, είναι εντελώς κρυφά από την δημόσια προβολή.

Η συνεχόμενη εξέλιξη του Zcash, όπως είναι η πρόσφατη αναβάθμιση με κωδική ονομασία "Overwinter network" και η εργασία προς την κατεύθυνση των Z συναλλαγών με την χρήση πορτοφολιών χαμηλής απαίτησης πόρων συστήματος για χρήση σε κινητά τηλέφωνα, φέρνει βελτιώσεις οι οποίες παρέχουν ιδιωτικότητα στις συναλλαγές με ένα παρόμοιο τρόπο που παρέχεται από το "μετρητό" χρήμα, αλλά με την ευκολία που παρέχει ένα ψηφιακό νόμισμα και το πλεονέκτημα του να μην εκδίδεται και ελέγχεται από κάποια κεντρική αρχή.

2.0 Ethereum

Το Ethereum κατά τον ίδιο τρόπο επέκτεινε τις δυνατότητες των αποκεντρωμένων εφαρμογών και την χρήση τους στην τεχνολογία blockchain, επιτρέποντας στους προγραμματιστές πρόσβαση σε μία ανοιχτή πλατφόρμα για την ανάπτυξη εφαρμογών, έξυπνων συμβολαίων και πολλών ακόμη.
Από την λευκή βίβλο του Ethereum:

> *Αυτό το οποίο το Ethereum προτίθεται να παράσχει είναι ένα δίκτυο blockchain με μια ενσωματωμένη πλήρως λειτουργική γλώσσα προγραμματισμού που μπορεί να χρησιμοποιηθεί για την δημιουργία "έξυπνων συμβολαίων" τα οποία θα επιτρέπουν στους χρήστες να εκτελέσουν τις λειτουργίες που περιγράφηκαν παραπάνω, καθώς και άλλα πολλά τα οποία δεν έχουμε ακόμη φανταστεί, απλώς γράφοντας μερικές γραμμές κώδικα.*

Με βάση αυτό το όραμα το Ethereum έχει γίνει μια κινητήριος δύναμη σε πολλές πτυχές ανάπτυξης της τεχνολογίας blockchain καθώς και της βιομηχανίας ψηφιακών νομισμάτων. Το Ethereum παρέχει την δυνατότητα για ένα κόσμο όπου τα περισσότερα (αν όχι όλα) τα συστήματα θα μπορούσαν να επωφεληθούν από την τεχνολογία blockchain καθώς και των πλεονεκτημάτων που πηγάζουν από αυτήν. Είτε πρόκειται για την ψηφιοποίηση περιουσιακών στοιχείων η την δυνατότητα να πραγματοποιηθούν αρχικές προσφορές νομίσματος (ICO), έχει δώσει την δύναμη στους χρήστες να δημιουργήσουν ένα νέο διαδίκτυο το είδος του οποίου θα μας φαινόταν αδιανόητο πριν από μερικά χρόνια.

Παρόλα ταύτα τα προβλήματα κλιμάκωσης παραμένουν, και υπάρχει έντονος προβληματισμός για το αν θα μπορέσουν τελικά να επιλυθούν. Περιορισμένο στις περίπου 15-20 συναλλαγές το δευτερόλεπτο, το Ethereum είναι απλά πολύ αργό για να κάνει το όραμα του πραγματικότητα.

'Οπως θα περιγράψουμε σε αυτό το κείμενο, το Zel σκοπεύει να λύσει το πρόβλημα της κλιμάκωσης οριστικά, κάνοντας το όραμα του Ethereum πράξη. Έχουμε δημιουργήσει ένα οικοσύστημα προϊόντων και εφαρμογών προκειμένου να επιτύχουμε αυτόν τον σκοπό, επικεντρωνόμενοι στην προσβασιμότητα και την χρηστικότητα.

3.0 Zel

Οι τεχνολογίες Zel εργάζονται σε συμβιωτική σχέση μεταξύ τους αλλά και με τεχνολογίες εκτός του οικοσυστήματος Zel. Το Zel είναι σχεδιασμένο ως ένα ανοιχτό σύστημα που συνεργάζεται με τεχνολογίες "κλειστού κώδικα". Βλέπε τμήμα 4.0 για τις θεμελιώδεις βάσεις του Zel.

4.0 Βασικές Λειτουργίες Zelcash

Στην επιφάνεια του το Zelcash είναι ένα "εξωρύξιμο" ψηφιακό νόμισμα που βασίζεται στα τεχνολογικά θεμέλια του κρυπτονομίσματος Zcash (πρότερα γνωστό ως Zerocash), το όποιο με την σειρά του βασίζεται στο bitcoin. Το Zelcash χρησιμοποιεί τον ίδιο αλγόριθμο κρυπτογράφησης με το Zcash, ο οποίος χρησιμοποιείται επίσης και από άλλα ψηφιακά νομίσματα που στοχεύουν στην ανωνυμία. Το γεγονός αυτό δημιουργεί ένα σχετικά μεγάλο δίκτυο προγραμματιστών από διαφορετικές ομάδες οι όποιοι με το πέρασμα του χρόνου προσθέτουν βελτιώσεις στο πρωτόκολλο ώστε συνεχώς να βελτιώνεται η λειτουργικότητα του.

Σε αντίθεση με το bitcoin, του οποίου οι ισχυρισμοί περί ανωνυμίας εχουν καταρριφθεί τα τελευταία χρόνια, το Zcash διασφαλίζει την ανωνυμία του χρήστη μέσω του πρωτοκόλλου zk-SNARKs (βλέπε τμήμα 4.2).
Με την ανωνυμία του τελικού χρήστη να είναι μία από τις θεμελιώδεις αρχές του αρχικού οράματος του bitcoin, κάθε βελτίωση και γενικά εξέλιξη της ιδέας της ιδιωτικότητας θα έπρεπε να τυγχάνει θερμής υποδοχής από τους κατόχους αλλά και τους χρήστες των ψηφιακών νομισμάτων ανωνυμίας. Το Zel έχει επιλέξει να κάνει χρήση των χαρακτηριστικών ανωνυμίας του Zcash προκειμένου να επιτύχει το όραμα της ανωνυμίας, και στοχεύει να αυξήσει την υιοθέτηση ενός τέτοιου χαρακτηριστικού διάμεσου ενός μεγάλου κλιμακούμενου δικτύου.

Το Zelcash παρέχει οικονομικό κίνητρο για την εμπλοκή στο αποκεντρωμένο δίκτυο κόμβων μας (ZelNodes), το όποιο θα αποτελεί ένα πραγματικά αποκεντρωμένο, κλιμακούμενο δίκτυο προγραμματισμού blockchain. Το οικονομικό κίνητρο αυτό παρέχεται διαμέσου ενός μεριδίου των ανταμοιβών Zel block, και εν τέλει δια μέσου διαφορετικών οικονομικών μοντέλων όπως είναι οι προμήθειες συναλλαγών, η χρέωση λειτουργίας για τις αποκεντρωμένες εφαρμογές (DApps), προμήθειες έξυπνων συμβολαίων και άλλα πολλά και άλλα στα πλαίσια της υλοποίησης του οράματος μας για ένα πανίσχυρο αποκεντρωμένο κλιμακούμενο δίκτυο.

4.1 T συναλλαγές

T_συναλλαγές είναι οι παραδοσιακές συναλλαγές που καταγράφονται στο blockchain του Bitcoin. Οι συναλλαγές αυτές πραγματοποιούνται μεταξύ διάφανων διευθύνσεων, γνωστών και ως T-διευθύνσεων, με αρχική προέλευση τους την τεχνολογία του Bitcoin. Οι συναλλαγές αυτές είναι οι πιο συχνά χρησιμοποιούμενες μεταξύ πορτοφολιών και ανταλλακτηρίων. Αυτό συμβαίνει διότι απαιτούν λιγότερη επεξεργαστική ισχύ προκειμένου να εκτελεστεί η συναλλαγή και μπορούν να πραγματοποιηθούν από κινητά τηλέφωνα και άλλες φορητές συσκευές.

4.2 Z συναλλαγές

Οι Z_συναλλαγές είναι θωρακισμένες ή ιδιωτικές. Αυτές αποστέλλονται μεταξύ Z_διευθύνσεων, επίσης γνωστών ως "θωρακισμένων διευθύνσεων." Το Zelcash τις κληρονόμησε από το Zcash και ως εκ τούτου επωφελείται από τις τεχνικές προόδους και εξελίξεις που πραγματοποιούνται στα πρωτόκολλα, η στις αναβαθμίσεις του δικτύου όπως το πρόσφατο Overwinter fork.

Εάν η αποστολή γίνεται από μία ή περισσότερες θωρακισμένες διευθύνσεις, η αξία της συναλλαγής/γων παραμένει απόρρητη. Μόνο όταν υπάρχει μία διαφανής διεύθυνση στο λαμβάνον άκρο η συναλλαγή θα πάψει να είναι απόρρητη. Αυτό θα έχει ως αποτέλεσμα να αποκαλυφθεί η αξία που παραλήφθηκε μόνο από την συγκεκριμένη διάφανη διεύθυνση στο δίκτυο. Η θωρακισμένη διεύθυνση αποστολής, καθώς και το ποσό που αυτή απέστειλε παραμένουν απόρρητα. Το πρωτόκολλο Zcash περιγράφει αυτή την διαδικασία με λεπτομέρεια:

Η αξία σε Zcash είναι είτε διάφανη είτε θωρακισμένη.

- Οι μεταφορές διάφανης αξίας λειτουργούν ουσιαστικά όπως το Bitcoin και έχουν τις ίδιες ιδιότητες ιδιωτικότητας.
- Η θωρακισμένη αξία μεταφέρεται από σημειώματα, τα οποία αναφέρουν ένα ποσό και ένα κλειδί πληρωμής. Το κλειδί πληρωμής είναι μέρος της διεύθυνσης πληρωμής, η οποία συνιστά έναν προορισμό όπου μπορούν να σταλούν τα σημειώματα. Όπως με το Bitcoin, αυτό συσχετίζεται με ένα ιδιωτικό κλειδί το οποίο μπορεί να χρησιμοποιηθεί για να ξοδέψει τα νομίσματα που αποστέλλονται στην διεύθυνση. Στο Zcash αυτό ονομάζεται κλειδί ξοδέματος.

Κάθε γραμμάτιο έχει μία κρυπτογραφικά συσχετιζόμενη υποχρέωση γραμμάτιου και έναν μοναδικό ακύρωτη (ώστε να υπάρχει πάντα μια σχέση 1:1:1 μεταξύ γραμμάτιων, υποχρεώσεων γραμμάτιων και ακυρωτών).
Για την εκτέλεση του ακυρωτή απαιτείται το συσχετιζόμενο κλειδί ξοδέματος. Είναι ανέφικτο να συσχετιστεί η υποχρέωση σημειώματος με τον αντιστοιχούντα ακυρωτή χωρίς την γνώση του κλειδιού ξοδέματος.

Μια συναλλαγή μπορεί να περιέχει διάφανες εισαγωγές, εξαγωγές και κείμενα κώδικα, τα οποία όλα δουλεύουν όπως στο πρωτόκολλο Bitcoin. Επίσης περιέχει μια αλληλουχία από μια zero η περισσοτέρων JoinSplit περιγραφών. Κάθε μία από αυτές περιγράφει μια JoinSplit μεταφορά η λαμβάνει μια διάφανη αξία και έως δυο εισερχόμενων γραμμάτιων και παράγει μια διάφανη αξία έως δύο εξερχόμενων γραμμάτιων.

Οι ακυρωτές των εισερχόμενων γραμμάτιων αποκαλύπτονται (εμποδίζοντας τους να χρησιμοποιηθούν ξανά) και η υποχρεώσεις των εξερχόμενων γραμμάτιων

αποκαλύπτονται (επιτρέποντας τα να χρησιμοποιηθούν στο μέλλον). Κάθε JoinSplit περιγραφή περιλαμβάνει επίσης μια υπολογιστική σταθερά zk-SNARK, η οποία επιβεβαιώνει όλα τα κάτωθι ισχύουν πλην αμελητέας πιθανότητας:

- Η αξία που εισήχθη και εξήχθη είναι ίδια (ξεχωριστά για κάθε JoinSplit μεταφορά).
- Για κάθε εισαχθέν γραμμάτιο μη μηδενικής αξίας, κάποια αποκαλυφθείσα αξία υποχρέωσης υφίσταται για αυτό το γραμμάτιο.
- Ο επαληθευτής γνώριζε το απόρρητο κλειδί ξοδέματος των εισαχθέντων γραμμάτιων.
- Οι ακυρωτές και οι υποχρεώσεις γραμματίου είναι υπολογισμένα σωστά.
- Τα απόρρητα κλειδιά ξοδέματος των εισαχθέντων γραμμάτιων είναι κρυπτογραφικά συνδεδεμένα με μια υπογραφή καθ' όλη την διάρκεια της συναλλαγής, με τέτοιο τρόπο ώστε η συναλλαγή να μην μπορεί να τροποποιηθεί από ένα τρίτο μέρος το οποίο δεν γνωρίζει αυτά τα απόρρητα κλειδιά.
- Κάθε εξαχθέν γραμμάτιο παράγεται με τέτοιο τρόπο ώστε να είναι αδύνατο ο ακυρωτής του να έρθει σε σύγκρουση με τον ακυρωτή οποιουδήποτε άλλου γραμματίου.

Εκτός των διευθύνσεων zk-SNARK (θωρακισμένων διευθύνσεων), γίνεται επίσης έλεγχος ότι οι ακυρωτές των εισαχθέντων γραμματίων δεν έχουν ήδη αποκαλυφθεί (δηλαδή ότι δεν έχουν ήδη ξοδευτεί).

Μια διεύθυνση πληρωμής περιλαμβάνει δυο δημόσια κλειδιά:

1. ένα κλειδί πληρωμής που ταιριάζει με το γραμμάτιο που αποστέλλεται προς την διεύθυνση, και
2. ένα κλειδί μετάδοσης για χρήση στο σχέδιο απόρρητου κλειδιού ασύμμετρης κρυπτογράφησης.

“Απόρρητο κλειδί” σημαίνει ότι τα κρυπτογραφικά κείμενα δεν αποκαλύπτουν με βάση ποιο κλειδί κρυπτογραφήθηκαν, εκτός από τον κάτοχο του αντιστοιχούντος απορρήτου κλειδιού, το οποίο εν προκειμένου ονομάζεται *viewing key .* Αυτό το μοναδικό κλειδί χρησιμοποιείται ώστε να επικοινωνούν τα κρυπτογραφημένα εξερχόμενα γραμμάτια με τον τελικό αποδέκτη τους, ο οποίος μπορεί να χρησιμοποιήσει viewing key για να σκανάρει το δίκτυο για γραμμάτια που προορίζονται για αυτόν και να τα αποκρυπτογραφήσει.

Η βάση των ιδιοτήτων απορρήτου του Zcash έχει ως εξής: Όταν ένα γραμμάτιο ξοδεύεται, αυτός που το ξόδεψε αποδεικνύει ότι κάποια υποχρέωση προς αυτό έχει αποκαλυφθεί, χωρίς να αποκαλύπτει ποια ήταν αυτή. Αυτό σημαίνει ότι ένα γραμμάτιο το οποίο ξοδεύτηκε δεν μπορεί να συνδεθεί με την συναλλαγή για την όποια αυτό δημιουργήθηκε.

Από μια αντίπαλη οπτική γωνία, το σύνολο των δυνατοτήτων ενός γραμμάτιου, περιλαμβάνει όλα τα προηγούμενα γραμμάτια τα όποια ο αντισυμβαλλόμενος ούτε ελέγχει ούτε γνωρίζει εάν έχουν ξοδευτεί. Αυτό έρχεται σε αντίθεση με άλλες προτάσεις για απόρρητα συστήματα πληρωμών όπως είναι το CoinJoin η το CryptoNote τα οποία βασίζονται στην ανάμιξη ενός περιορισμένου αριθμού συναλλαγών και ως εκ τούτου έχουν πολύ μικρότερα ίχνη εντοπισμού των συναλλασσόμενων γραμματίων.

Οι ακυρωτές είναι απαραίτητοι για να αποφευχθεί το διπλό ξόδεμα: κάθε γραμμάτιο έχει έναν μόνο έγκυρο ακυρωτή, συνεπώς η απόπειρα ξοδέματος ενός γραμματίου δυο φορές θα είχε ως αποτέλεσμα να αποκαλυφθεί ο ακυρωτής δυο φορές, προκαλώντας την απόρριψη της δεύτερης συναλλαγής.

4.3 Απόδειξη-Παροχής-Έργου (POW)

Καθώς ο Nakamoto βελτίωνε την εργασία την εργασία του Adam Back το Hashcash, δημιούργησε ένα σύστημα επικύρωσης που βασίζεται σε κρυπτογραφικό κατακερματισμό αντί της εμπιστοσύνης ενός κεντρικού συστήματος. Ακολουθώντας την χρήση του αλγορίθμου εξόρυξης Bitcoin SHA-256 από τον Nakamoto, ήρθε η εφαρμογή του αλγορίθμου Scrypt από το Litecoin, ακολουθούμενο από το Dash και το Ethereum που χρησιμοποίησαν το X11 και το Ethash, αντίστοιχα. Πρόσφατες μετεξελίξεις (της αρχικής ιδέας του X11, το οποίο είναι μια αλληλουχία αλγορίθμων κατακερματισμού όπου η εξαγωγή του ενός γίνεται η εισαγωγή του επόμενου) είναι οι αλγόριθμοι εξόρυξης X13, X15, και X17.

Η αρχική πρόθεση ήταν η εξόρυξη του Bitcoin(BTC) να πραγματοποιείται με επεξεργαστές οικιακού υπολογιστή (CPU) αναθέτοντας τον κατακερματισμό καθώς και τις ψήφους στους επεξεργαστές. Λίγο αργότερα ωστόσο, αναπτύχθηκαν επιλυτές που χρησιμοποιούσαν την επεξεργαστική ισχύ των καρτών γραφικών (GPU). Καθώς η τιμή του Bitcoin ανέβαινε, αυξανόταν επίσης και το κίνητρο της εξόρυξης του, και έγινε βιώσιμο για προγραμματιζόμενο υλικό όπως είναι οι FPGA κάρτες να χρησιμοποιηθούν για την εξόρυξη Bitcoin. Αυτές είχαν ένα πλεονέκτημα και επί των επεξεργαστών (CPU) και επί των καρτών γραφικών (GPU). Ακλουθώντας την ανάπτυξη των FPGA ήρθε η ανάπτυξη του επί αυτού του σκοπού κατασκευασμένου υλικού εξόρυξης (ASIC), το οποίο λόγω της αποδοτικότητας του σύντομα κυριάρχησε στο δίκτυο Bitcoin, καθιστώντας το πλέον ασύμφορη την εξόρυξη Bitcoin με CPU, GPU ακόμα και με FPGA.

Χτίζοντας στην ιδέα της ένωσης πολλών αλγορίθμων εξόρυξης μαζί σε μια αλληλουχία που πρωτοεμφανίστηκε στον X11, σύντομα ήλθε ο X13, X15, X17. Αυτές οι αλληλουχίες λειτουργούν παρόμοια αλλά ενσωματώνουν περισσότερους αλγορίθμους εξόρυξης, με σκοπό να γίνει πιο δύσκολη η κατασκευή ενός ASIC που θα τους εκτελεί. Το Zelcash βασίστηκε στην τεχνολογία απορρήτου του Zcash και επωφελείται από τα πλεονεκτήματα που πηγάζουν από αυτό. Όμως όπως πολλά κρυπτονομίσματα που βασίζονται στο Zcash, κληρονόμησε την μέθοδο επίτευξης συναίνεσης Απόδειξης Παροχής Έργου (POW). Λόγω της ανόδου της τιμής του Zcash έγινε οικονομικά βιώσιμο να δημιουργηθούν ASICs για τον αλγόριθμο εξόρυξης Equihash 200, 9. Καθώς πολλά κρυπτονομίσματα (BTCZ, BTG, SAFE κ.α.) μετακινήθηκαν σε μία διαφορετική σειρά παραμέτρων, άρχισαν να επιδεικνύον ανθεκτικότητα ενάντια στους κατασκευαστές ASIC.

Η ομάδα προγραμματισμού του Zel προγραμμάτισε την αλλαγή του αλγόριθμου εξόρυξης Equihash 200,9 με τον επίσης POW αλγόριθμο εξόρυξης X16R. Η ανάπτυξη προχωρούσε κανονικά, ενσωματώνοντας την κρυπτογραφική μέθοδο zk-SNARK μέσα στον αλγόριθμο κατακερματισμού ώστε να ξεκινήσει το δοκιμαστικό δίκτυο, όταν

έγκυρες πληροφορίες εμφανιστήκαν ότι FPGAs και ASICs αναπτύσσονταν για τον αλγόριθμο X16R που θα μπορούσαν να είναι 100 έως 1000 φορές πιο αποτελεσματικά από τις GPUs.

Καθώς μαχόμαστε εναντίον των ASICs, οι πρόσφατες εξελίξει στο υλικό FPGA συνιστούν μια ακόμη πρόκληση. Παρότι η εξόρυξη με επεξεργαστή ηλεκτρονικού υπολογιστή θα ήταν ιδανική, κατανοούμε ότι το μεγαλύτερο μέρος της κοινότητας εξόρυξης χρησιμοποιεί κάρτες γραφικών, και εμείς επίσης διατηρούμε μια κάποια επιπλέον συμπάθεια για τις GPU. Συνεπώς καταλήγουμε στο ότι αντιμαχόμαστε τους ASICs και προσπαθούμε για διασώσουμε την εξόρυξη με κάρτες γραφικών.

Η ανάπτυξη του αλγορίθμου X16R για το Zelcash συνεπώς σταμάτησε. Η ποσότητα της εργασίας που απαιτήθηκε, χωρίς τελικά να καταφέρουμε το επιθυμητό αποτέλεσμα της ανθεκτικότητας στους ASIC, ήταν πολύ μεγάλη.

Για τους λόγους που προαναφέρθηκαν, το Zelcash θα αλλάζει αλγοριθμους κατακερματισμού σε τροποποιημένο Equihash με N,K σταθερές του 144 και 5, την ίδια δηλαδή προσέγγιση που και άλλα κρυπτονομίσματα έχουν υιοθετήσει πρόσφατα. Αυτό θα είναι μια προσωρινή λύση ώστε να παραμείνουμε ανθεκτικοί στους ASICs και τους FPGAs έως ότου μπορέσουμε να βρούμε μια πιο μόνιμη λύση. Λύσεις αναπτύσσονται συνεχώς ώστε να κρατηθεί η εξόρυξη με κάρτες γραφικών ζωντανή, και ως εκ τούτου να προστατευτεί το όραμα της αποκέντρωσης της διαδικασίας εξόρυξης. Μία τέτοια ιδέα είναι το progPOW, το οποίο θα μελετηθεί και θα συζητηθεί από την ομάδα του Zel τις ερχόμενες εβδομάδες. Εις βάθος αναλύσεις μελλοντικών αλγορίθμων και οι στρατηγικές ανθεκτικότητας σε ASIC/FPGA που θα ακολουθηθούν, θα περιγραφούν σε μελλοντικές εκδόσεις αυτού του κειμένου.

Καθώς το Zel στοχεύει στην δημιουργία ενός αποκεντρωμένου δικτύου, είναι μόνο λογικό να θέλουμε να διατηρήσουμε αποκεντρωμένη την διαδικασία εξόρυξης του Zelcash το οποίο με την σειρά του χρηματοδοτεί την ανάπτυξη του αποκεντρωμένου δικτύου ZelDev. Θα συνεχίσουμε τον αγώνα μας ώστε να παραμείνουμε ανθεκτικοί στους ASICs. Η αναβάθμιση του αλγορίθμου εξόρυξης θα έχει ολοκληρωθεί μέχρι το τέλος του Ιουλίου 2018.

Τέλος, ο αλγόριθμος δυσκολίας θα φύγει από το παλιό Digishield V3 στο Zawy's LWMA. Ο αλγόριθμος του Zawy (LWMA) χαρίζει πολύ μεγαλύτερη σταθερότητα στους χρόνους block και προσαρμόζεται πολύ πιο γρήγορα από το Digishield V3, χαρίζοντας μεγάλη αύξηση στην ταχύτητα κατακερματισμού. Στις μετρήσεις μας το Zawy's LWMA, είναι 10 φορές πιο γρήγορο στην εύρεση block απ' ότι το Digishield V3. Ο νέος αλγόριθμος δυσκολίας θα μας βοηθήσει να αμυνθούμε ενάντια σε επιθέσεις κατά του δικτύου καθώς το Zel κυκλοφορεί περισσότερα προϊόντα διότι πιθανότατα θα αυξηθεί και η ισχύς κατακερματισμού του δικτύου καθώς το δίκτυο μεγαλώνει. Αυτή η κίνηση θα είναι μέρος της αναβάθμισης του δικτύου Zel τον Ιούλιο του 2018.

4.4 Ανταμοιβή Block

Στο ξεκίνημα του το Zelcash είχε μία αργή εκκίνηση της τάξεως των 5,000 blocks, αφότου εξορύχθηκε το ταμείο προγραμματιστών (Dev Fund) από το block 5,000 και έπειτα η ανταμοιβή εύρεσης block είναι 150 Zelcash της οποίας το 100% πηγαίνει στους PoW miners. Καθώς η εξέλιξη των κόμβων Zel (ZelNodes) πλησιάζει, η ανταμοιβή block θα τροποποιηθεί προκειμένου να δοθεί στην απόκτηση και διατήρηση κόμβου. Τα ακριβή ποσά θα προταθούν από την ομάδα του Zel και θα αποφασιστούν από την κοινότητα κατά τις εβδομάδες που θα ακολουθήσουν την κυκλοφορία αυτού του κειμένου.

Η πρόθεση της προσαρμοσμένης ανταμοιβής block θα είναι να εξασφαλίσει ικανό κέρδος εξίσου για την mining κοινότητα καθώς και για τους ιδιοκτήτες κόμβων Zel. Αυτή η αναλογία θα είναι μεταβαλλόμενη ανάλογα με τις συνθήκες ώστε να εξασφαλίζει μία δίκαιη ανταμοιβή προς όλους.

Η ανταμοιβή block θα μειώνεται στο ήμισυ κάθε 2.5 χρόνια, μετρώντας από το αρχικό block (genesis block).

4.5 Κόμβοι Zel (ZelNodes)

Η έννοια των κόμβων Zel συνελήφθη κατόπιν μίας συζήτησης, για το πως θα μπορούσε να κλιμακωθεί μια αποκεντρωμένη πλατφόρμα προγραμματισμού, εφαρμογών και έξυπνων συμβολαίων, όπως είναι το δίκτυο Ethereum. Προγράμματα όπως το Lisk το Neo και άλλα έχουν καταφέρει να το επιτύχουν. Αντιμετωπίζουν τον κίνδυνο ωστόσο να απομακρυνθούν από το όραμα της "αποκέντρωσης" στην προσπάθεια τους να προσφέρουν προσβάσιμη τεχνολογία blockchain.

Το Ethereum είναι αποκεντρωμένο, συνεπώς αντιμετωπίζει προβλήματα κλιμάκωσης, όπως όλα τα μέχρι στιγμής αποκεντρωμένα δίκτυα. Με DApps όπως οι Crypto Kitties να γονατίζουν το δίκτυο του Ethereum, το αποτέλεσμα είναι αργές ακριβές συναλλαγές που αυξάνουν κατά πολύ το κόστος των έξυπνων συμβολαίων που εκτελούνται εντός του δικτύου.

Το γεγονός αυτό δεν είναι μόνο θέμα κόστους. Θα μπορούσε να προκαλέσει δυσλειτουργίες σε DAOs και πολλές άλλες εφαρμογές που λειτουργούν εντός του δικτύου, πράγμα ανεπίτρεπτο στον δικτυωμένο κόσμο τον οποίον ζούμε. Με την δημιουργία ενός υποκινούμενου δικτύου παρόμοιας δομής με του DASH, το Zelcash μας επιτρέπει να δημιουργήσουμε ένα πραγματικά αποκεντρωμένο και διανεμημένο

δίκτυο κόμβων. Αυτό θα επέτρεπε ένα κλιμακούμενο δίκτυο, παρόμοιο με του Ethereum, με πολύ μεγαλύτερη δυνατότητα εξυπηρέτησης όγκου συναλλαγών.

Αυτό θα καταστεί εφικτό χρησιμοποιώντας τις ZelChains (sidechains) επιτρέποντας περισσότερες συναλλαγές ανά δευτερόλεπτο.

Αυτό είναι απαραίτητο εάν σκοπεύουμε να περάσουμε σε ένα αποκεντρωμένο διαδίκτυο. Το Ethereum δεν μπορεί στην παρούσα να κλιμακωθεί ώστε να καλύψει αυτές τις απαιτήσεις. Η Uber μας δίνει ένα πραγματικό παράδειγμα: με 12 δρομολόγια το δευτερόλεπτο, το δίκτυο θα κορεζόταν, πράγμα που σημαίνει ότι ένας ανταγωνιστής όπως η Lyft δε θα μπορούσε να λειτουργήσει στο ίδιο δίκτυο. Παρότι το όραμα του Vitalik Buterin ήταν για 1 εκατομμύριο συναλλαγές το δευτερόλεπτο (TPS), προς το παρόν είναι 15-20. Με επινοήσεις ωστόσο όπως είναι ο τεμαχισμός (sharding) υπό εξέλιξη, είναι πιθανό ότι το Ethereum κάποια στιγμή θα καταφέρει να επιτύχει αυτά τα νούμερα.

Δεν θέλουμε να μπούμε στον πειρασμό να αναφέρουμε τυχαία νούμερα χωρίς πραγματικές αποδείξεις, αλλά θεωρητικά (με βάση το μοντέλο που έχουμε εκπονήσει) το δίκτυο Zel θα μπορέσει να επιτύχει υψηλότερα TPS από το δίκτυο Ethereum σε λιγότερο χρόνο. Με την κλιμάκωση που θα επιτευχθεί μέσω των ZelNodes, θα μπορούσαμε θεωρητικά να ανταγωνιστούμε το δίκτυο της VISA σε συναλλαγές ανά δευτερόλεπτο (TPS). Σημειώστε ότι αυτή είναι μία εκτίμηση για πάνω από 1000 TPS, αλλά είναι μόνο αυτό, μια εκτίμηση. Θέλουμε να αποδείξουμε την τεχνολογία μας πριν αναφέρουμε νούμερα τα οποία ενδέχεται να αλλάξουν, αλλά θεωρούμε την εκτίμηση μας πολύ συντηρητική.

Δε θα ανακοινώσουμε οριστικά νούμερα συναλλαγών ανά δευτερόλεπτο (TPS) έως ότου το κυρίως δίκτυο μας (Mainnet) έχει ενεργοποιηθεί και δοκιμαστεί για αρκετούς μήνες ώστε να μπορούμε να παρουσιάσουμε ρεαλιστικά νούμερα τα οποία δεν θα είναι υπερβολές η χωρίς να έχουν δοκιμαστεί στην πράξη.

4.6 Οικονομικά κόμβων Zel

Ενεργοί κόμβοι που χρησιμοποιούνται για να ασφαλίσουν το δίκτυο ενός νομίσματος καθώς και τις διαδικασίες συναλλαγών, υπάρχουν από την εποχή ίδρυσης του ψηφιακού νομίσματος DASH. Έκτοτε, πολλά προγράμματα έχουν προσθέσει την πλατφόρμα των Κυρίως Κόμβων (Masternodes-MNs) ως μέσω το οποίο δίνει κίνητρο στους κατόχους νομισμάτων, κλειδώνει την παροχή του νομίσματος και ενδυναμώνει την εξόρυξη και την αγοραπωλησία. Κάποια πρότζεκτ ήταν επιτυχή στην ενσωμάτωση των Masternodes, ενώ κάποια άλλα νεώτερα μικρής κεφαλαιοποίησης νομίσματα χρησιμοποιούσαν το δόλωμα των Masternodes υποσχόμενα μη ρεαλιστικές επιστροφές ώστε να επιτύχουν γρήγορη αύξηση της κοινότητας τους και της κεφαλαιοποίησης τους

η οποία συνήθως οδηγούσε σε απάτες εξόδου η απλά την κατάρρευση της αξίας του νομίσματος. Για να δημιουργήσουμε ένα υγιές και αποκεντρωμένο περιβάλλον Masternodes (ZelNodes) για αυτό το πρότζεκτ, οι εγγυήσεις και οι ανταμοιβές θα σχεδιαστούν ώστε να είναι ρεαλιστικές και να αξίζουν τον χαρακτηρισμό της μακροπρόθεσμης επένδυσης.

Οι ZelNodes θα είναι μια δομή κόμβων τριών επιπέδων, που θα απαιτούν τρία διαφορετικά επίπεδα εγγυήσεων και απαιτήσεων υλικού, και που θα παράγουν τριών διαφορετικών επιπέδων ανταμοιβές. Οι ανταμοιβές των κόμβων Zel θα διανέμονται στους κατόχους του κόμβου δίνοντας τους ένα κομμάτι από κάθε εξορυχθέν block και σε μια αναλογία του 25% για τους ZelNodes και 75% για τους PoW miners. Αυτά τα νούμερα ενδέχεται στο μέλλον να αλλάξουν καθώς είναι απαραίτητο να διατηρηθεί μιας μεγάλης κλίμακας και μεγάλης υπολογιστικής ισχύος, αποκεντρωμένο δίκτυο (βλέπε τμήμα 4.5) Ένας κόμβος Zel επίσης θα απαιτεί μεγάλη διαθεσιμότητα, συνεπώς ένας σταθερός χρόνος λειτουργίας (uptime) είναι απαραίτητος για να ληφθεί η ανταμοιβή κόμβου. Τα απαιτούμενα ποσοστά χρόνου διαρκούς λειτουργίας του κόμβου θα δημοσιευτούν καθώς πλησιάζουμε στην ενεργοποίηση των Zelnodes.

Συνιστώμενες απαιτήσεις υλικού συστήματος ZelNode:

Spec. Type	Zelnode Βασικό	ZelNode Σούπερ	ZelNode BAMF
Επεξεργαστής (CPU)	2 Πυρήνες	4 Πυρήνες	8 Πυρήνες
Μνήμη (RAM)	4GB	8GB	32GB
Σκληρός δίσκος (SSD)	50GB	150GB	600GB
Εύρος Ζώνης	2.5TB	4TB	6TB

Για την ώρα τα τρία επίπεδα κόμβων Zel ονομάζονται ZelNode Βασικό (χαμηλότερες απαιτήσεις), ZelNode Σούπερ (μεσαίες απαιτήσεις), και ZelNode BAMF (υψηλότερες απαιτήσεις). Κάθε κόμβος Zel έχει απαιτήσεις Προσωπικού Εικονικού Εξυπηρετητή (VPS), το οποίο μεταφράζεται σε συνδρομητική υπηρεσία επί πληρωμή. Όλοι οι κόμβοι Zel θα έχουν προαπαιτούμενο χρόνο διαρκούς λειτουργίας, συνεπώς οι χρόνοι και τα χαρακτηριστικά του συστήματος θα μετρηθούν από το Zel ώστε να διασφαλιστεί η συμμόρφωση με τους κανόνες και ότι η ανταμοιβή λειτουργίας κόμβου θα αποδοθεί μόνο σε όσους την δικαιούνται.

Προτεινόμενη δομή εγγυήσεων και ανταμοιβής:

Επίπεδο κόμβου	Εγγύηση [Zel]	Ανταμοιβή % (25% από κάθε block)
ZelNode Βασικό	10,000	15%
ZelNode Σούπερ	25,000	25%
ZelNode BAMF	100,000	60%

Το μεγάλο εύρος του ύψους της εγγύησης επιτρέπει σε έναν μεγάλο αριθμό ατόμων να συμμετάσχει στο σύστημα κόμβων Zel εφόσον το επιθυμούν, και το μη γραμμικό σύστημα εγγυήσεων και ανταμοιβής εγγυάται ότι για παράδειγμα 10 βασικοί κόμβοι Zel δε θα μπορούν να κερδίσουν περισσότερα από έναν κόμβο BAMF.

Το οικονομικό μοντέλο σχεδιάστηκε με εκτιμώμενη τιμή Zel στο 1$ μέχρι το τέλος του 2018. Όντας μια μακροπρόθεσμη επένδυση το συσχετιζόμενο κόστος διατήρησης ενός κόμβου Zel είναι σχετικά ασήμαντο και θεωρείται υποθετική επένδυση, με τον ίδιο τρόπο με τον οποίο γίνεται η υποθετική εξόρυξη ενός νέου ψηφιακού νομίσματος, όπου το άμεσο οικονομικό κέρδος δεν είναι στις προθέσεις του επενδυτή.

Με την ικανότητα να αλλάξει ελαφρώς η ανταμοιβή block προς τα πάνω ή προς τα κάτω, η ομάδα του Zel έχει την δυνατότητα να διατηρήσει ένας ορισμένο αριθμό κόμβων στο δίκτυο αυξάνοντας την ανταμοιβή εάν ο συνολικός αριθμός των κόμβων πέσει κάτω από κάποιο επίπεδο, η μειώνοντας τις ανταμοιβές στην περίπτωση πληθώρας κόμβων. Αυτή η ενέργεια θα εκτελείται εξαιρετικά σπάνια και μόνο σαν τελευταία λύση ώστε να διασφαλιστεί η οικονομική ισορροπία στο δίκτυο Zel.

5.0 Διπλές οικονομίες

Το Zelcash είναι ο μηχανισμός συναλλαγών της πλατφόρμας Zeldev. Συσχετιζόμενες διαδικασίες, αμοιβές και υπηρεσίες θα συνδέονται απευθείας με την υποδομή του Zeldev και θα απαιτούν το νόμισμα του Zel, διεξάγουμε έρευνα ωστόσο για πιθανές μακροπρόθεσμες εξελίξεις περί ενός "διπλού οικονομικού μοντέλου". Καθώς το αποκεντρωμένο ανταλλακτήριο (DEX) και οι αποκεντρωμένες εφαρμογές (DApps) αναπτύσσονται, το όραμα μίας οικονομίας βασιζόμενης σε παροχή υπηρεσιών, καθώς και η στηριγμένη στο νόμισμα Zel δομή, θα πρέπει να αναπτυχθούν αμφότερες.

Η κατανόηση της ανάγκης ύπαρξης ενός στιβαρού δικτύου από miners, κόμβους και προγραμματιστές θα ισχυροποιήσει το Zelcash καθώς και την πλατφόρμα Zeldev. Καθώς προχωρά η ανάπτυξη του αποκεντρωμένου ανταλλακτηρίου (DEX) και των αποκεντρωμένων εφαρμογών (DApps), η ανάγκη να χρηματοδοτηθούν και να συντηρηθούν οι προγραμματιστές είναι απαραίτητη. Κατανοώντας ότι αυτό είναι κάτι το όποιο πρέπει να ληφθεί υπόψη, η ύπαρξη ενός ιδρύματος που θα παρέχει οικονομική στήριξη είναι το κλειδί για την εμπλοκή της κοινότητας σε μακροπρόθεσμα μοντέλα χρηματοδότησης.

6.0 Τεχνολογίες Zel

Οι τεχνολογίες Zel εργάζονται σε μια ποικιλία πρότζεκτ και εφαρμογών επιπρόσθετα του Zelcash. Όλα αυτά συνυπάρχουν και αλληλεπιδρούν σε συμβιωτική σχέση εντός του οικοσυστήματος Zel.

Το πρότζεκτ ιδρύθηκε πάνω στην ιδέα της δημιουργίας ενός αποκεντρωμένου δικτύου blockchain παρόμοιου με το δίκτυο του Ethereum, με όμως με μεγαλύτερη δυνατότητα εξυπηρέτησης συναλλαγών χάρη στην συναίνεση που θα επιτυγχάνεται μεταξύ των ενεργών κόμβων Zel. Εκτελώντας παρόμοια λειτουργία αλυσίδας με αυτή του Ethereum, οι αλυσίδες του ZelDev θα ονομάζονται αλυσίδες Zel (ZelChains). Οι ZelChains θα λειτουργούν σαν πλευρικές αλυσίδες σε ένα τύπου Lisk περιβάλλον, επιτρέποντας σε αυτά τα blockchains να επικοινωνούν μεταξύ τους όταν αυτό απαιτείται, αλλά χαρίζοντας επίσης και την δυνατότητα για την εκτέλεση μεγαλύτερο όγκου συναλλαγών και με όλα τα πλεονεκτήματα που παρέχει ένα πραγματικά αποκεντρωμένο δίκτυο.

Αυτό τοποθετεί το Zel στην θέση να:

- λύσει τα θέματα κλιμάκωσης που αντιμετωπίζει το Ethereum και παρόμοια πρότζεκτ, και
- να επιτρέψει αποκεντρωμένες εφαρμογές, έξυπνα συμβόλαια, αποκεντρωμένα oracles, συστήματα ψηφοφορίας κλπ, όλα αναπτυσσόμενα με κλιμακούμενο τρόπο.

Με αυτή την ώθηση, (που ξεκίνησε από τον Satoshi Nakamoto), απομακρυνόμαστε από το συγκεντρωτικό διαδίκτυο που γνωρίζαμε όλοι λίγα χρόνια πριν (και χρησιμοποιούμε ακόμα), σε ένα αποκεντρωμένο διαδίκτυο και κόσμο.

Άλλα πρότζεκτ όπως το ZelTreZ, ZelPay, Zel ID, και άλλα, μας επιτρέπουν να δημιουργήσουμε αυτό το οικοσύστημα, αναπτύσσοντας τεχνολογίες για το μέλλον.

6.1 Πορτοφόλι Zel (ZelTreZ)

Το ZelTreZ είναι μία πλατφόρμα που αναδύθηκε από την επιθυμία της ομάδας για μια καλύτερη πλατφόρμα πορτοφολιού απ' ότι προσφερόταν στην παρούσα στιγμή στον χώρο του ανοιχτού λογισμικού. Το Zel καταπιάστηκε με την δημιουργία ενός διπλής λειτουργίας πορτοφολιού, Χαμηλών πόρων (lite) καθώς και πλήρους κόμβου (full-node), το οποίο αρχικός περιλάμβανε μόνο το Zelcash. Σχεδιάστηκε για να δώσει στον

χρήση την επιλογή να επιλέξει ποιες δυνατότητες λειτουργίας χρειάζεται. Με το ξεκίνημα της ανάπτυξης τους, αρχίσαμε να συνειδητοποιούμε τις δυνατότητες της πλατφόρμας και ως εκ τούτου η ιδέα αναπτύχθηκε και καρποφόρησε σε αυτό που είναι σήμερα. Το ZelTrez είναι τώρα ένα πορτοφόλι πολλαπλών νομισμάτων που προσφέρει ελαφριά και πλήρους κόμβου λειτουργία ανάλογα με τις ανάγκες του χρήστη.

Σχεδιασμένο να προσφέρει ευκολία στην χρήση με ένα ευχάριστο και ελαφρύ περιβάλλον εργασίας, το ZelTreZ αναπτύσσεται σε μια πύλη για τον κόσμο των κρυπτονομισμάτων. Την παρούσα στιγμή υποστηρίζει τα εξής 16 ψηφιακά νομίσματα: Zelcash (ZEL), Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), Zcash (ZEC), BitcoinZ (BTCZ), Hush (HUSH), Ravencoin (RVN), Binance (BNB), BitCore (BTX), 0x (ZRX), OmiseGO (OMG), Zilliqa (ZIL), Basic Attention Token (BAT), Golem (GNT), BitcoinGold (BTG), Stox (STX), Civic (CVC), Zen (ZEN), Komodo (KMD), Zcoin (XZC), Safecoin (SAFE) και Snowgem (XSG), με νέα νομίσματα να ενσωματώνονται κάθε δύο εβδομάδες.

Με ενημερώσεις και βελτιώσεις ασφαλείας το ZelTreZ χρησιμοποιεί κρυπτογράφηση για να κρατά τους χρήστες ασφαλείς, επιτρέποντας την δημιουργία λογαριασμών χωρίς να αποθηκεύεται καμία πληροφορία του χρήστη απομακρυσμένα. Καθώς η ανάπτυξη του Zel συνεχίζεται, η έναρξη της πλατφόρμας ZelDev θα αναδείξει το αποκεντρωμένο μας δίκτυο προγραμματισμού διαμέσου του ZelTreZ στην μορφή του ZelDex, του αποκεντρωμένου μας ανταλλακτηρίου ψηφιακών νομισμάτων το οποίο θα προσφέρεται εγγενώς εντός του ZelTreZ.

Εκτός από μία βιτρίνα για (DApps), το ZelTreZ είναι επίσης μια πύλη για προγραμματιστές και μαθητές μέσω της οποίας μπορούν να εισέλθουν στον χώρο της blockchain τεχνολογίας προγραμματισμού και να αρχίσουν να υλοποιούν τις δικές τους εφαρμογές και λύσεις. Προς το παρόν διαθέσιμο για Windows, Linux, και MacOS, το ZelTreZ στο άμεσο μέλλον θα γίνει εφαρμογή έξυπνου τηλεφώνου για Android και iOS και πρόσθετο για τον περιηγητή Chrome, επιτρέποντας τις πρόσβαση στον λογαριασμό του χρήστη από διαφορετικές συσκευές και λειτουργικά συστήματα χωρίς να αποθηκεύεται καμία πληροφορία του λογαριασμού χρήστη στην υποδομή μας.

6.2 Ταυτότητα Zel (Zel ID)

Το ταυτότητα Zel (Zel ID) είναι ένα σύστημα επαλήθευσης που σχεδιάστηκε να επιτρέπει στους χρήστες να διατηρούν πλήρη έλεγχο επί των ψηφιακών τους ταυτοτήτων. Το Zel ID δίνει την δυνατότητα στους χρήστες του να διατηρούν καταγραφές περιουσιακών στοιχείων, ιατρικούς φακέλους και άλλες πληροφορίες σε ένα αποκεντρωμένο κρυπτογραφημένο δίκτυο, αντί να τα έχουν αποθηκευμένα σε έναν κεντρικό εξυπηρετητή η τυπωμένα σε χαρτί. Αυτό θα χαρίσει στον χρήση έλεγχο επί

των προσωπικών που περιουσιακών, ιατρικών η άλλων δεδομένων και θα προστατεύσει την ιδιωτικότητα που τόσο πολύ λείπει στον σύγχρονο ψηφιακό μας κόσμο.

Το Zel ID τροφοδοτείται από τις ίδιες λύσεις ασφαλείας που πρωτοπαρουσιάστηκαν από την Authparty, ένα υιοθετημένο από το Bitcoin σύστημα ταυτοποίησης το οποίο αναπτύχθηκε από το μέλος της ομάδας Zel, Matthew Reichardt. Το Zel ID επιτυγχάνει ταυτοποίηση "zero-proof" με τη χρησιμοποίηση υπογραφών που παράγονται από τα δημόσια και ιδιωτικά κλειδιά του πορτοφολιού σας. Αυτό ουσιαστικά καταργεί την ανάγκη για έλεγχο ταυτότητας δύο στοιχείων (2FA), μιας και η ταυτοποίηση απαιτεί κηδεμονική (custodial) πρόσβαση στο πορτοφόλι σας. Το πορτοφόλι σας σε αυτή την περίπτωση (εν προκειμένου το ZelTreZ), καθίσταται εξίσου σημαντικό με ένα κινητό τηλέφωνο η μία σύνδεση διαδικτύου.

Δημιουργούνται μοναδικές ταυτότητες επαλήθευσης, που ονομάζονται *Personas*, και χρησιμοποιούνται για επαλήθευση "for zero-proof" σε τρίτους παρόχους και υπηρεσίες.

Το μητρώο Zel παρέχει πρόσβαση "διεπαφής προγραμματισμού εφαρμογών" (API) προς το πρωτόκολλο επαλήθευσης Zel ID. Μέσω της παραχθείσας Persona, μια νέα ταυτότητα που ονομάζεται "οντότητα" (*Entity)* δημιουργείται αυτόματα και προσκολλάται στην Persona. Με αυτόν το τρόπο, μια υπηρεσία τρίτου μέρους που επαληθεύεται μέσω του Zel ID θα είχε τρεις βαθμίδες διαχωρισμού από την πραγματική ταυτότητα του πορτοφολιού, επιτρέποντας διαφορετικές Personas ενώ ταυτόχρονα θα εξασφάλιζε την δυνατότητα της ανωνυμίας του χρήστη.

6.3 Πληρωμές Zel (ZelPay)

Ένα απλό αλλά απαραίτητο πρόγραμμα το, ZelPay θα μπορούσε να χρησιμοποιηθεί σε τερματικό POS, σε καταστήματα καθώς και σε πρόσθετα (plugins) ηλεκτρονικών καταστημάτων. Το ZelPay σχεδιάζεται να δώσει στον τελικό χρήστη ευκολία χειρισμού και διαφάνεια, προσφέροντας τις επιχειρήσεις προμήθεια έως 1% επί της συναλλαγής.

Το πλεονέκτημα του ZelPay είναι μια ενοποιημένη εφαρμογή που προσφέρει ευκολία χρήσης εξίσου στο κατάστημα καθώς και στο διαδίκτυο, και η οποία χαρίζει στους ιδιοκτήτες επιχειρήσεων υψηλής ποιότητας στατιστικά στοιχεία πωλήσεων, ώστε να τους βοηθήσει να αναπτύξουν την επιχείρηση τους. Το ZelPay θα σχεδιαστεί έτσι ώστε να επιτρέπει στις επιχειρήσεις να αποδέχονται όχι μόνο όλα τα κρυπτονομίσματα του ZelTreZ, αλλά ενδεχομένως και ψηφιακά νομίσματα που είναι υποστηριζόμενα από το δολάριο, ευρώ, λίρα Αγγλίας, γιέν η χρυσό και ασημί (πχ USDT κ.α.). Αυτό θα επέτρεπε

το πιο εύκολο και πιο ελεύθερο εμπόριο υποστηριζόμενο από την δυνατότητα για υψηλότερο αριθμό συναλλαγών ανά δευτερόλεπτο (TPS) σε σχέση με άλλες λύσεις κρυπτονομισμάτων

Το ZelPay θα υποστηρίζει επικοινωνίες κοντινού πεδίου (NFC) και σάρωση κωδικού QR ώστε να διευκολύνει τις ανέπαφες συναλλαγές μέσω της εφαρμογής ZelTreZ για κινητά τηλέφωνα, παρέχοντας μια απροβλημάτιστη και εύκολη λειτουργία για τον πελάτη αλλά και τον έμπορο.

Μια υποθετική εφαρμογή για το ZelPay και άλλες εφαρμογές blockchain.

Έχουμε ήδη βιώσει την υιοθέτηση των αυτοεξυπηρετούμενων ραφιών σε σουπερ μάρκετ, μειώνοντας την ανάγκη για πολυάριθμους υπαλλήλους. Αντ' αυτού μόλις ένας απαιτείται για να επιτηρεί την σωστή λειτουργία των μηχανημάτων και ότι επαληθεύεται η ταυτότητα όσων αγοράζουν αλκοολούχα ποτά. Για να πάμε την ιδέα παραπέρα, οι πωλήσεις χωρίς προσωπικό δοκιμάζονται από την Amazon και άλλες εταιρίες, και αυτά τα συστήματα έχουν ήδη υιοθετηθεί σε κάποιες πόλεις.

Αυτό επιτυγχάνεται μέσω μια διαδικασίας που ακούγεται περίπλοκη αλλά στην πραγματικότητα δεν είναι. Ο αγοραστής σκανάρει τον κωδικό QR για να μπει στο κατάστημα, αυτό είναι το καλάθι αγορών του. Μόλις ο αγοραστής εισέρθει, επιλέγει τα προϊόντα που επιθυμεί και τα αποθέτει πάνω στον πάγκο εξόφλησης. Ο πάγκος διαβάζει τα αυτοκόλλητα RFID που είναι κολλημένα στα προϊόντα, δημιουργεί έναν νέο κωδικό QR code η επιτρέπει μια ανέπαφη πληρωμή NFC, και ο πελάτης αφού πληρώσει ηλεκτρονικά του επιτρέπεται να αποχωρήσει με τα προϊόντα. Αυτό το σύστημα θα μπορούσε να βελτιωθεί, αλλά μας δίνει ένα πολύ καλό παράδειγμα του πως η τεχνολογία μπορεί να βελτιώσει την εμπειρία του πελάτη και να μειώσει το κόστος για τις επιχειρήσεις.

6.4 Πλατφόρμα Zel (ZelDev)

Το ZelDev θα σχεδιαστεί με επίκεντρο τους προγραμματιστές, καθιστώντας την εργασία στην τεχνολογία blockchain όσο τον δυνατόν πιο εύκολα προσβάσιμη. Θα το επιτύχουμε αυτό δίνοντας πρόσβαση στους προγραμματιστές στο ZelSDK και BDK, τα οποία επιτρέπουν την εύκολη υιοθέτηση του blockchain σε νέα ή ήδη υπάρχοντα πρότζεκτ. Θα υπάρχουν κάποια έτοιμα template για ZelChains τα οποία θα βοηθήσουν τους προγραμματιστές να αλληλεπιδράσουν με αυτά χρησιμοποιώντας Javascript. Επίσης templates έξυπνων συμβολαίων και ψηφιακών νομισμάτων θα είναι διαθέσιμα, επιτρέποντας την συγγραφή έξυπνων συμβολαίων σε Javascript. Αυτό χαμηλώνει τον πήχη εισόδου για τους προγραμματιστές, καθότι η Javascript είναι η πιο ευρέως

χρησιμοποιούμενη γλώσσα προγραμματισμού. Για να διαχειριστούν τις συναλλαγές νομισμάτων θα διαμοιράζονται σε ξεχωριστές αλυσίδες block, που όποτε απαιτείται, θα επικοινωνούν με την κυρίως αλυσίδα του ZelDev. Αυτό επίσης θα επιτρέψει διαχείριση μεγαλύτερου όγκου συναλλαγών, και θα μπορούσε να μειώσει τις επιπτώσεις όταν πχ μια συγκεκριμένη αλυσίδα βρίσκεται υπό συντήρηση

Τεχνικές λεπτομέρειες που αφορούν την πλατφόρμα ZelDev και των προϊόντων απευθείας συσχετιζόμενων με αυτήν, θα κοινοποιηθούν σε μεταγενέστερη ημερομηνία.

6.5 Αλυσίδες Zel (ZelChains)

Η κυρίως αλυσίδα ZelDev μαζί με τις πλευρικές αλυσίδες Zel (sidechains) είναι αλυσίδες μπλοκ (blockchains) που θα λειτουργούν στο δίκτυο κόμβων Zel. Αυτό θα επιτρέψει την πραγματική αποκέντρωση με κλιμακούμενο τρόπο, καθώς οι κόμβοι αυτοί θα έχουν πολύ υψηλό χρόνο αδιάλειπτης λειτουργίας με αποτέλεσμα να δημιουργούνται νέοι δίοδοι όταν μια αλυσίδα καθίσταται κορεσμένη, και θα αυξήσει επίσης την δυνατότητα των συνολικών συναλλαγών ανά δευτερόλεπτο (TPS) που το δίκτυο Zel θα μπορεί να διεκπεραιώσει.

6.6 Ανταλλακτήριο Zel (ZelDex)

Την παρούσα στιγμή τα μεγαλύτερα ανταλλακτήρια ψηφιακών νομισμάτων είναι συγκεντρωτικά (centralized). Στις περισσότερες περιπτώσεις ο χρήστης δεν κατέχει ο ίδιος τα ιδιωτικά του κλειδιά για τα πορτοφόλια των ανταλλακτηρίων, και ως εκ τούτου δεν του ανήκουν τα κρυπτονομίσματα που περιέχονται στον λογαριασμό του.

Παρότι τα συγκεντρωτικά ανταλλακτήρια παρέχουν μια πολύ καλύτερη εμπειρία χρήστη καθώς και περισσότερες συναλλαγές ανά δευτερόλεπτο, τα αποκεντρωμένα ανταλλακτήρια βελτιώνονται. Με νέα ανταλλακτήρια που προσφέρουν έλεγχο του χρήστη επί των κλειδιών του, είμαστε στην αρχή της επανάστασης της αγοράς των ανταλλακτηρίων. Το βασικό ζήτημα που εμποδίζει την μαζική υιοθέτηση των αποκεντρωμένων ανταλλακτηρίων είναι τα ζητήματα κλιμάκωσης, εν μέρει λόγω της ελλιπούς υποδομής τους.

Το ZelDex θα χτιστεί στην κορυφή του ZelDev ως δείγμα γραφής των δυνατοτήτων του δικτύου Zel. Το περιβάλλον χρήσης θα σχεδιαστεί να είναι απλό στην περιήγηση αλλά και αρκετά περίπλοκο για προχωρημένους χρήστες. Με ενσωμάτωση απευθείας στο ZelTreZ, καθώς και σαν ξεχωριστή πλατφόρμα διαδικτύου και εφαρμογή κινητού τηλεφώνου, το ZelDex στοχεύει να γίνει το πρώτο αποκεντρωμένο ανταλλακτήριο

(Dex) με μαζική υιοθέτηση στον χώρο.

Επίσης τα ανοιχτά αιτήματα API θα επιτρέψουν στους προγραμματιστές να χρησιμοποιήσουν το ZelDex στις εφαρμογές τους για την ανταλλαγή tokens και νομισμάτων.

6.7 Κατάστημα Dapp

Το κατάστημα ZelDapp θα είναι ένα κεντρικό hub για αποκεντρωμένες και μερικές συγκεντρωτικές εφαρμογές, με χαμηλό πήχη εισόδου, με ορισμένους κανόνες και κανονισμούς ώστε να διασφαλιστεί η νομιμότητα. Το app store είναι σχεδιασμένο έτσι ώστε να επιτρέπει στους προγραμματιστές να έχουν πρόσβαση σε μια μεγάλη βάση χρηστών σε λύσεις cross-platform. Το ZelTreZ λειτουργεί σαν sandbox για αυτές τις Dapps, ώστε να μπορέσουν να λειτουργήσουν σε σύντομο χρόνο χωρίς να χρειάζεται να περιμένουν την έγκριση από συγκεκριμένες εταιρίες.

Το ZelDapps διαφέρει από άλλες προτάσεις blockchain λόγω της χαμηλής δυσκολίας εκμάθησης. Το framework θα είναι προσβάσιμο μέσω του Κιτ Ανάπτυξης Λογισμικού (SDK), το οποίο πιθανότατα θα είναι Javascript, και πιθανώς και άλλες γλώσσες καθώς η πλατφόρμα θα αναπτύσσεται. Η χρησιμοποίηση μιας εξαιρετικά δημοφιλούς γλώσσας προγραμματισμού θα εξασφαλίσει εύκολη πρόσβαση σε εργαλεία ανάπτυξης και προσβασιμότητα σε έναν ευρύ αριθμό επαγγελματιών αλλά και ερασιτεχνών προγραμματιστών.

Στις τεχνολογίες Zel, πιστεύουμε ότι οι άνθρωποι θα πρέπει να είναι σε θεση να επικοινωνούν ελευθέρα και χωρίς περιορισμούς. Για τον σκοπό αυτό, ένας messenger θα δημιουργηθεί ως το πρώτο DApp. Ίσως να ακολουθηθεί και από μια πλατφόρμα μέσων κοινωνικής δικτύωσης που επιτρέπει στους ανθρώπους να εκφράζουν την γνώμη τους χωρίς λογοκρισία (εντός των ορίων του νόμου).

Θα υπάρχει μια μικρή, έως καθόλου, αμοιβή στο κατάστημα ZelDApp. Θα σχεδιαστεί ως μια δωρεάν και ελεύθερη αγορά που θα επιτρέπει σε προγραμματιστές να προσεγγίσουν χρήστες.

7.0 Ηγεσία και συνεισφορές στην Λευκή Βίβλο

Ιδρυτής - Miles Manley
Συνέταιρος και προγραμματιστής - Lumi Ibishi
Συνέταιρος και επικεφαλής προγραμματισμού - Tadeas Kmenta
Επικεφαλής σύμβουλος- Daniel Keller
Διευθυντής προγράμματος και σύμβουλος - Parker Honeyman

Σεβασμός προς: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Την ημέρα δημιουργήθηκε, το Bitcoin άλλαξε για πάντα την οικονομική ελευθερία για εκείνους που επιλέγουν ένα διαφορετικό μονοπάτι. Η τεχνολογία είναι ο μεγάλος ισορροπιστής, για όλους όσους δημιουργούν το μέλλον, σε χαιρετίζουμε!

-Η ομάδα Zel

8.0 Το μέλλον του Zel

Το Zel θα είναι ένα αέναο, εξελισσόμενο οικοσύστημα. Η ομάδα είναι προσηλωμένη στο όραμα της αλλαγής του κόσμου μέσω της blockchain τεχνολογίας και των κρυπτονομισμάτων. Για τον σκοπό αυτό, το Zel θα εμπλέκεται προνοητικά σε νέες αναδυόμενες τεχνολογίες, προγράμματα και εξελίξεις ηγεσίας. Πιστεύουμε ότι ο χώρος χρειάζεται ηγέτες που θα εισάγουν νέες τεχνολογίες, και θα θέλαμε να βρισκόμαστε στην πρώτη γραμμή.

Προχωρώντας μπροστά η ομάδα του Zel θα:

- συνεχίσει να αναπτύσσει νέες τεχνολογίες βασισμένες στο μοντέλο του Zelcash σε προγράμματα κλειστού καθώς και ανοιχτού κώδικα.
- συνεταιριστεί με άλλους στο χώρο ώστε να εξασφαλιστεί ότι το πρότζεκτ θα παραμείνει στην πρώτη γραμμή των εξελίξεων.
- αναπτύξει και διατηρήσει μια κοινότητα γύρω από την πλατφόρμα Zel που θα καθοδηγεί τις αξίες και τις αποδόσεις του επιχειρηματικού μοντέλου.
- αναπτύξει και διατηρήσει ένα φιλανθρωπικό παρακλάδι του ιδρύματος Zel για την ανακούφιση αναξιοπαθούντων μέσω της χρήσης αναδυόμενων τεχνολογιών.

9.0 Γλωσσάριο

Altcoin-- Ένα κρυπτονόμισμα που δεν είναι το Bitcoin.

ASIC (application-specific integrated circuit)-- Κυκλώματα πυριτίου ειδικά σχεδιασμένα για να εκτελούν μια συγκεκριμένη διεργασία, εν προκειμένου εξόρυξη Bitcoin και λοιπών κρυπτονομισμάτων, τρέχοντας συγκεκριμένους αλγόριθμους (πχ SHA-256)

Τεχνολογία Cross-chain-- Επιτρέπει σε δύο διαφορετικές αλυσίδες μπλοκ (blockchains) να ανταλλάσουν πληροφορίες και κρυπτονομίσματα ταυτόχρονα.

DASH-- Ένας τύπος κρυπτονομίσματος που βασίζεται στο λογισμικό του, το οποίο προσφέρει στοιχεία ανωνυμίας, παλαιότερα γνωστό ως XCoin (XCO) και Darkcoin.

Χρήμα Fiat-- Νομίσματα (χαρτονόμισμα-κέρματαα) χωρίς αξία που πηγάζει από αντίκρισμα σε χρυσό η άλλα πολύτιμα μέταλλα, που όμως είναι καθορισμένα ως νόμιμο μέσω πληρωμής και εκδίδονται από κεντρική τράπεζα κράτους η ένωσης.

JoinSplit-- δεδομένα που περιλαμβάνονται σε μια συναλλαγή που περιγράφει μια *JoinSplit* μεταφορά, πχ μια θωρακισμένη μεταφορά. Αυτού του είδους οι μεταφορές αξίας είναι το κύριο χαρακτηριστικό εκτέλεσης συναλλαγών του Zcash.

Litecoin (LTC)-- Κρυπτονόμισμα που δημιουργήθηκε από τον πρώην υπάλληλο της Google, Charlie Lee το 2011. Επιτρέπει γρηγορότερη επεξεργασία σε χαμηλότερο κόστος.

NEO-- Αναφέρεται στο κρυπτονόμισμα και το όνομα του πρώτου blockchain ανοιχτού κώδικα της Κίνας. Όπως το Ethereum, μπορεί να εκτελέσει έξυπνα συμβόλαια και DApps, σε κάπως πιο συγκεντρωτικό περιβάλλον.

Overwinter fork-- Το πρώτο σκληρό fork Zcash το οποίο επέλυσε ζητήματα δικτύου και επιδόσεων, μεταξύ άλλων, ώστε να ενδυναμώσει το δίκτυο για μελλοντικές αναβαθμίσεις.

Multi Signature (multisig)-- Οι διευθύνσεις Multisig επιτρέπουν σε πολλαπλά μέρη να απαιτούν άνω του ενός κλειδιού για να εκτελεστεί μια συναλλαγή. Οι διευθύνσεις Multisig έχουν μεγαλύτερη ανθεκτικότητα στην κλοπή.

Ιδιωτικό κλειδί-- Το ιδιωτικό κλειδί είναι ένα νήμα δεδομένων που δίνει σε έναν

χρήστη έλεγχο επί ενός δημοσίου κλειδιού και μιας διεύθυνσης ώστε να μπορεσει εκτελεστεί μια συναλλαγή κρυπτονομίσματος.

Proof of Stake (PoS)-- Ένας αλγόριθμος που ανταμείβει τους συμμετέχοντες που λύνουν δύσκολα κρυπτογραφικά πάζλ ώστε να επιτευχθεί η διανεμημένη συναίνεση. Το PoS έχει μικρότερη ενεργειακή κατανάλωση από το PoW.

Proof of Work (PoW)-- Ένας αλγόριθμος που ανταμείβει το πρώτο άτομο, η ομάδα ατόμων (pool), που λύνουν δύσκολα κρυπτογραφικά πάζλ ώστε να επιτευχθεί η διανεμημένη συναίνεση.

Z-cash-- Ένα από τα πρώτα κρυπτονομίσματα ιδιωτικού απορρήτου.

Zel ID-- Ένα σύστημα ταυτοποίησης που δημιουργεί μια online Persona για τον χρήστη, για να χρησιμοποιηθεί σε όλες τις εκφάνσεις τις ζωής, και προς κάθε σύστημα που απαιτεί ταυτοποίηση φυσικού προσώπου.

ZelChains-- Οι πλευρικές αλυσίδες που θα τρέχουν στο δίκτυο του Zelcash ώστε να παράσχουν αξιοποιήσιμη υπολογιστική ισχύ και κλιμάκωση στους προγραμματιστές αποκεντρωμένων εφαρμογών.

ZelDev-- Η πλατφόρμα μέσω της οποίας οι προγραμματιστές DApps θα αλληλεπιδρούν με την blockchain του Zelcash διαμέσου εύκολου στην χρήση SDK και BDK περιβάλλοντος.

ZelDex-- Ένα αποκεντρωμένο ανταλλακτήριο (DEX) που δημιουργήθηκε από το Zelcash για να τρέχει στο αποκεντρωμένο δίκτυο και θα παρέχεται μέσω του ZelTreZ αλλά και κατά μόνας μέσω ιστοσελίδας η εφαρμογής κινητού τηλεφώνου.

Κόμβοι Zel (ZelNodes)-- Ένα πολυεπίπεδο υποκινούμενο δίκτυο υπολογιστικής ισχύος για χρήση από τους προγραμματιστές DApps, και την διακίνηση ψηφιακών νομισμάτων, το οποίο είναι στιβαρό, κλιμακούμενο και πραγματικά αποκεντρωμένο.

ZelTreZ-- Η πλατφόρμα που φέρει το Zelcash. Το ZelTreZ είναι ένα κρυπτογραφημένο πολυ-πορτοφόλι κρυπτονομισμάτων, τα οποίο θα φιλοξενεί το Dex, θα διαχειρίζεται τα πορτοφόλια των ZelNodes και θα περιέχει το Dapp Store.

zk-SNARK-- Ένα πρωτόκολλο ιδιωτικού απορρήτου που πρωτοξεκίνησε από το Zcash και επιτρέπει τις θωρακισμένες συναλλαγές που διασφαλίζουν την ανωνυμία των συναλλασσόμενων μερών.(Βλέπε το whitepaper του Zcash για τεχνική ανάλυση)

Πηγές

[1] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system

[2] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Zcash Protocol Specification Version 2017.0-beta-2.5.

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: decentralised Anonymous Payments from Bitcoin

[4] Vitalik Buterin and the Ethereum Project: A Next-Generation Smart Contract and decentralised Application Platform, Ethereum

[5] Tron Black and Joel Weight: X16R ASIC Resistant Design