Cardano Whitepaper

(μετάφραση από το Greek Cardano Community - SapioPool Team)

Εισαγωγή

Κίνητρο

Το Cardano είναι ένα έργο που ξεκίνησε το 2015 ως μία προσπάθεια να αλλάξει τον τρόπο σχεδιασμού και ανάπτυξης των κρυπτονομισμάτων. Η συνολική εστίαση πέρα από ένα συγκεκριμένο σύνολο καινοτομιών είναι η παροχή ενός πιο ισορροπημένου και βιώσιμου οικοσυστήματος που να ανταποκρίνεται καλύτερα στις ανάγκες των χρηστών του, καθώς και σε άλλα συστήματα που επιδιώκουν «ενσωμάτωση» (“integration”).

Στο πνεύμα πολλών έργων ανοιχτού κώδικα, ο Cardano δεν ξεκίνησε με έναν ολοκληρωμένο χάρτη πορείας ή ακόμη και μια έγκυρη «Λευκή Βίβλο» (“whitepaper”). Αντίθετα, αγκάλιασε μια συλλογή από αρχές σχεδιασμού, βέλτιστες πρακτικές μηχανικής και τρόπους εξερεύνησης. Αυτά περιλαμβάνουν τα ακόλουθα:

- Διαχωρισμός λογιστικής και υπολογισμού σε διαφορετικά επίπεδα.
- Εφαρμογή βασικών στοιχείων σε πολύ αρθρωτό λειτουργικό κώδικα.
- Μικρές ομάδες ακαδημαϊκών και προγραμματιστών που ανταγωνίζονται σε έρευνα που ελέγχεται από ομότιμους.
- Βαριά χρήση διεπιστημονικών ομάδων, συμπεριλαμβανομένης της έγκαιρης χρήσης ειδικών του InfoSec.
- Απαιτείται γρήγορη ακολουθία μεταξύ των Λευκών Βίβλων, εφαρμογή και νέα έρευνα για τη διόρθωση ζητημάτων που ανακαλύφθηκαν κατά την αναθεώρηση.
- Δημιουργία βασισμένη στη δυνατότητας αναβάθμισης συστημάτων μετά την ανάπτυξη, χωρίς καταστροφή του υπάρχοντος δικτύου.
- Ανάπτυξη ενός αποκεντρωμένου (“decentralized”) μηχανισμού χρηματοδότησης για μελλοντικές εργασίες.
- Μια μακροπρόθεσμη άποψη για τη βελτίωση του σχεδιασμού των κρυπτονομισμάτων ώστε να μπορούν να λειτουργούν σε κινητές συσκευές με μια λογική και ασφαλή εμπειρία για τον χρήστη.
- Προσέγγιση των ενδιαφερομένων μερών πιο κοντά στις λειτουργίες και τη συντήρηση του κρυπτονομίσματος τους.
- Αναγνωρίζοντας την ανάγκη παρουσίασης πολλαπλών στοιχείων στο ίδιο καθολικό (“ledger”).
- Περίληψη συναλλαγών για να συμπεριληφθούν προαιρετικά μεταδεδομένα (“metadata”), ώστε να ανταποκρίνονται καλύτερα στις ανάγκες των παλαιών συστημάτων.
- Μαθαίνοντας από σχεδόν 1.000 altcoins και αγκαλιάζοντας λειτουργίες που έχουν νόημα.
- Υιοθέτηση μιας διαδικασίας βάσει των προτύπων εμπνευσμένη από την Ομάδα Μηχανικής του Διαδικτύου (“Internet Engineering Task Force”) χρησιμοποιώντας μια συγκεκριμένη βάση για να κλειδώσει το τελικό πρωτόκολλο σχεδιασμού.
- Εξερεύνηση των κοινωνικών στοιχείων του εμπορίου.
- Εύρεση ενός υγιούς μέσου για την αλληλεπίδραση των ρυθμιστικών αρχών με το εμπόριο χωρίς να διακυβεύονται ορισμένες βασικές αρχές που κληρονομούνται από το Bitcoin.

Από αυτό το μη-δομημένο σύνολο ιδεών, η ομάδα που εργάζεται στο Cardano άρχισε να εξερευνεί τόσο τη λογοτεχνία γύρω από τα κρυπτονομίσματα όσο και να δημιουργούν ένα σύνολο εργαλείων αφαίρεσης. Το αποτέλεσμα αυτής της έρευνας είναι η εκτεταμένη βιβλιοθήκη εγγράφων του IOHK, πολλά αποτελέσματα έρευνας, όπως αυτή η πρόσφατη επισκόπηση γλώσσας scripts, καθώς και μια οντολογία έξυπνων συμβολαίων (“Ontology of Smart Contracts”) και το έργο Scorex. Τα μαθήματα απέδωσαν μια εκτίμηση για την ασυνήθιστη και κατά καιρούς αντιπαραγωγική ανάπτυξη της βιομηχανίας κρυπτονομισμάτων.

Πρώτον, σε αντίθεση με τα επιτυχημένα πρωτόκολλα όπως το TCP/IP, υπάρχει λίγη «διαστρωμάτωση» (“layering”) στο σχεδιασμό των κρυπτονομισμάτων. Υπήρξε η επιθυμία να διατηρηθεί μια ενιαία έννοια της συναίνεσης σχετικά με τα δεδομένα και τα γεγονότα που καταγράφονται σε ένα ενιαίο καθολικό, ανεξάρτητα από το εάν έχει νόημα.

Για παράδειγμα, το Ethereum αντιμετώπισε τεράστια πολυπλοκότητα προσπαθώντας να γίνει ένας παγκόσμιος υπολογιστής, αλλά υποφέρει από ασήμαντες ανησυχίες που ενδέχεται να καταστρέψουν την ικανότητα του συστήματος να λειτουργεί ως μία αποθήκη αξίας. Πρέπει το πρόγραμμα όλων να είναι ένας πολίτης πρώτης κατηγορίας ανεξάρτητα από την οικονομική του αξία, το κόστος διατήρησής του ή τις κανονιστικές του συνέπειες;

Δεύτερον, υπάρχει μικρή εκτίμηση για τα προηγούμενα αποτελέσματα στην επικρατούσα κρυπτογραφική έρευνα. Για παράδειγμα, το Bitshares “Delegated Proof of Stake” θα μπορούσε εύκολα και αξιόπιστα να δημιουργήσει τυχαίους αριθμούς χρησιμοποιώντας τη ρίψη νομίσματος με εγγυημένη παράδοση αποτελέσματος, η οποία είναι μια τεχνική γνωστή από τη δεκαετία του 1980 (βλ. Το σεμιναριακό έγγραφο των Rabin και Ben-Or).

Τρίτον, τα περισσότερα altcoins (με μερικές αξιοσημείωτες εξαιρέσεις όπως το Tezos) δεν έχουν κάνει καμία πρόβλεψη για μελλοντικές ενημερώσεις. Η ικανότητα επιτυχούς ώθησης ενός «μαλακού» ή «σκληρού πιρουνιού» (“soft or hard fork”) είναι καθοριστικής σημασίας για τη μακροπρόθεσμη επιτυχία οποιουδήποτε κρυπτονομίσματος.

Ως επακόλουθο, οι χρήστες δεν μπορούν να δεσμεύσουν πόρους αξίας εκατομμυρίων δολαρίων σε πρωτόκολλα όπου ο «χάρτης πορείας» (“roadmap”) και οι παράγοντες πίσω από αυτούς είναι εφήμεροι, μικροί ή ριζοσπαστικοί. Πρέπει να υπάρχει μια αποτελεσματική διαδικασία μέσω της οποίας μπορεί να διαμορφωθεί κοινωνική συναίνεση γύρω από ένα όραμα για την εξέλιξη του υποκείμενου πρωτοκόλλου. Εάν αυτή η διαδικασία είναι εξαιρετικά επαχθής, ο κατακερματισμός θα μπορούσε να διαλύσει την κοινότητα.

Τέλος, το χρήμα είναι τελικά ένα κοινωνικό φαινόμενο. Στην προσπάθεια «ανωνυμοποίησης» και αποσύνδεσης κεντρικών παραγόντων, το Bitcoin και οι σύγχρονοι του έχουν απορρίψει επίσης την ανάγκη για σταθερές ταυτότητες, μεταδεδομένα και φήμη στις εμπορικές συναλλαγές. Η προσθήκη αυτών των δεδομένων μέσω κεντρικών λύσεων αφαιρεί την δυνατότητα ελέγχου (“audit”), τη συνολική διαθεσιμότητα και το αμετάβλητο - το οποίο είναι το βασικό σημείο της χρήσης ενός blockchain.

Τα παλαιά (“legacy”) χρηματοοικονομικά συστήματα όπως αυτά που αποτελούνται από SWIFT, FIX και ACH είναι πλούσια σε μεταδεδομένα συναλλαγών. Δεν αρκεί να γνωρίζουμε πόση αξία μετακινήθηκε μεταξύ λογαριασμών, το ρυθμιστικό πλαίσιο συχνά αναζητά την απόδοση των εμπλεκόμενων φορέων, πληροφορίες συμμόρφωσης, αναφορά ύποπτης δραστηριότητας και άλλα αρχεία και ενέργειες. Σε ορισμένες περιπτώσεις, τα μεταδεδομένα είναι πιο σημαντικά από την ίδια τη συναλλαγή.

Ως εκ τούτου, φαίνεται λογικό να συναχθεί ότι ο χειρισμός των μεταδεδομένων θα μπορούσε να είναι εξίσου επιβλαβής με την παραχάραξη του νομίσματος ή την επανεγγραφή του ιστορικού συναλλαγών. Το να μην γίνεται καταγραφή αυτών που θέλουν να συμπεριλάβουν εθελοντικά αυτούς τους τομείς φαίνεται αντιπαραγωγικό για τη γενική υιοθέτηση και την προστασία των καταναλωτών.

Η συγκέντρωση της βασικής μας εξερεύνησης του χώρου της κρυπτογράφησης είναι δύο συλλογές πρωτοκόλλων. Αντίστοιχα, το αποδεδειγμένα ασφαλές “Proof of Stake” που ονομάζεται Cardano Settlement Layer (CSL) και ένα σύνολο πρωτοκόλλων που ονομάζονται Cardano Computation Layer (CCL).

Η σχεδιαστική μας έμφαση είναι να προσαρμόσουμε τις κοινωνικές πτυχές των κρυπτονομισμάτων, να δημιουργήσουμε στρώματα διαχωρίζοντας τη λογιστική της αξίας από τον περίπλοκο υπολογισμό και να αντιμετωπίσουμε τις ανάγκες των ρυθμιστικών αρχών στο πλαίσιο διαφόρων αμετάβλητων αρχών. Επιπλέον, όπου είναι λογικό, προσπαθούμε να ελέγξουμε προτεινόμενα πρωτόκολλα μέσω αξιολόγησης από ομοτίμους (“peer review”) και να ελέγξουμε τον κώδικα με βάση τις τυπικές προδιαγραφές.

Proof of Stake

Η χρήση του Proof of Stake σε ένα κρυπτονόμισμα είναι μια «καυτά» συζητημένη επιλογή σχεδιασμού, ωστόσο επειδή προσθέτει έναν μηχανισμό για την εισαγωγή ασφαλούς ψηφοφορίας, έχει μεγαλύτερη χωρητικότητα για κλιμάκωση (“scalability”) και επιτρέπει περισσότερα «εξωτικά» σχέδια κινήτρων, αποφασίσαμε να το οικειοποιηθούμε.

Το πρωτόκολλο μας Proof of Stake ονομάζεται Ouroboros και έχει σχεδιαστεί από μια εξαιρετικά ταλαντούχα ομάδα κρυπτογράφων από πέντε ακαδημαϊκά ιδρύματα με επικεφαλής τον καθηγητή Άγγελο Κιαγιά του Πανεπιστημίου του Εδιμβούργου. Η βασική καινοτομία που προσφέρει πέρα από το να αποδειχθεί ασφαλής χρησιμοποιώντας ένα αυστηρό κρυπτογραφικό μοντέλο είναι ένας αρθρωτός και ευέλικτος σχεδιασμός που επιτρέπει τη σύνθεση πολλών πρωτοκόλλων για την ενίσχυση της λειτουργικότητας.

Αυτή η αρθρωτότητα (“modularity”) επιτρέπει λειτουργίες όπως ανάθεση, πλευρικές αλυσίδες, εγγεγραμμένα σημεία ελέγχου, καλύτερες δομές δεδομένων για ελαφρούς πελάτες, διαφορετικές μορφές δημιουργίας τυχαίων αριθμών και ακόμη και διαφορετικές παραδοχές συγχρονισμού. Καθώς αναπτύσσεται ένα δίκτυο από χιλιάδες έως εκατομμύρια και ακόμη και δισεκατομμύρια χρήστες, οι απαιτήσεις του αλγόριθμου συναίνεσης θα αλλάξουν επίσης. Επομένως, είναι ζωτικής σημασίας να υπάρχει αρκετή ευελιξία για την αντιμετώπιση αυτών των αλλαγών και, ως εκ τούτου, να αποδεικνύεται μελλοντικά η καρδιά ενός κρυπτονομίσματος.

Κοινωνικά στοιχεία του χρήματος

Τα κρυπτονομίσματα είναι ένα πρωταρχικό παράδειγμα της κοινωνικής συνιστώσας του χρήματος. Όταν περιορίζεται η ανάλυση αποκλειστικά στην τεχνολογία, υπάρχει μικρή διαφορά μεταξύ Bitcoin και Litecoin και ακόμη λιγότερο μεταξύ Ethereum και Ethereum Classic. Ωστόσο, τόσο το Litecoin όσο και το Ethereum Classic διατηρούν μεγάλες κεφαλαιοποιήσεις στην αγορά και ισχυρές, δυναμικές κοινότητες καθώς και τις δικές τους κοινωνικές εντολές.

Μπορεί να υποστηριχθεί ότι ένα μεγάλο μέρος της αξίας ενός κρυπτονομίσματος προέρχεται από την κοινότητά του, τον τρόπο που χρησιμοποιεί το νόμισμα και το επίπεδο εμπλοκής της κοινότητας στην εξέλιξη του νομίσματος. Προχωρώντας τη σκέψη, νομίσματα όπως το Dash έχουν ενσωματώσει ακόμη και συστήματα απευθείας στο πρωτόκολλο για να εμπλέξουν την κοινότητά τους να αποφασίζει τι πρέπει να είναι προτεραιότητα για ανάπτυξη και χρηματοδότηση.

Η μεγάλη ποικιλία κρυπτονομισμάτων παρέχει επίσης στοιχεία για τα κοινωνικά τους στοιχεία. Οι διαφωνίες σχετικά με τη φιλοσοφία, τη νομισματική πολιτική ή ακόμα και μεταξύ των βασικών προγραμματιστών οδηγούν σε κατακερματισμό και πιρούνια (“forks”). Ωστόσο, σε αντίθεση με τους «αντιπάλους» των κρυπτονομισμάτων, τα νομίσματα (“fiat”) των υπερδυνάμεων τείνουν να επιβιώνουν από πολιτικές μετατοπίσεις και τοπικές διαφωνίες χωρίς νομισματική κρίση ή μαζική έξοδο.

Επομένως, φαίνεται ότι υπάρχουν στοιχεία παλαιών συστημάτων που λείπουν από τον κλάδο των κρυπτονομισμάτων. Υποστηρίζουμε - και το έχουμε εντάξει στον χάρτη πορείας του Cardano - ότι οι χρήστες ενός πρωτοκόλλου χρειάζονται κίνητρα για να κατανοήσουν την κοινωνική σύμβαση πίσω από το πρωτόκολλό τους και να έχουν την ελευθερία να προτείνουν αλλαγές με παραγωγικό τρόπο. Αυτή η ελευθερία επεκτείνεται σε κάθε πτυχή ενός συστήματος ανταλλαγής αξιών, από το να αποφασίζει πώς πρέπει να ρυθμίζονται οι αγορές έως ποια έργα θα πρέπει να χρηματοδοτηθούν. Ωστόσο, δεν μπορεί να διαμεσολαβηθεί μέσω κεντρικών φορέων ούτε να απαιτήσει κάποια ειδικά διαπιστευτήρια που θα μπορούσαν να επιλεγούν από μια καλά χρηματοδοτούμενη μειονότητα.

Το Cardano θα εφαρμόσει ένα σύστημα πρωτοκόλλων επικάλυψης που θα είναι κατασκευασμένο πάνω από το CSL για να καλύψει τις ανάγκες των χρηστών του.

Πρώτον, ανεξάρτητα από την επιτυχία ενός crowdsale στην ανάπτυξη bootstrap, τα χρήματα τελικά θα εξαφανιστούν. Ως εκ τούτου, το Cardano θα περιλαμβάνει ένα αποκεντρωμένο καταπίστευμα (“trust”) που θα χρηματοδοτείται από μονοτονικά μειωμένες χρεώσεις πληθωρισμού και συναλλαγών.

Οποιοσδήποτε χρήστης θα πρέπει να έχει το δικαίωμα να ζητά χρήματα από το καταπίστευμα από ένα σύστημα ψηφοφορίας και οι stakeholders του CSL ψηφίζουν ποιος γίνεται δικαιούχος. Η διαδικασία δημιουργεί έναν παραγωγικό βρόχο ανατροφοδότησης που εμφανίζεται σε άλλα κρυπτονομίσματα με συστήματα ταμείου / καταπίστευμα, όπως το Dash, ξεκινώντας μια συζήτηση για το ποιος πρέπει και δεν πρέπει να χρηματοδοτηθεί.

Οι συζητήσεις χρηματοδότησης επιβάλλουν μια σχέση μακροπρόθεσμων και βραχυπρόθεσμων στόχων, το κοινωνικό συμβόλαιο του κρυπτονομίσματος, τις προτεραιότητες και την πίστη στη δημιουργία αξίας

με συγκεκριμένες προτάσεις. Αυτή η συζήτηση σημαίνει ότι η κοινότητα αξιολογεί συνεχώς και συζητά τις πεποιθήσεις της έναντι πιθανών οδικών χαρτών.

Δεύτερον, η ελπίδα μας είναι ότι το Cardano θα συμπεριλάβει τελικά ένα επίσημο σύστημα βασισμένο σε blockchain για να προτείνει και να ψηφίζει τόσο μαλακά όσο και σκληρά "πιρούνια". Το Bitcoin με τη συζήτηση σχετικά με το μέγεθος του μπλοκ, το Ethereum με το "πιρούνι" DAO και πολλά άλλα κρυπτονομίσματα πέρασαν από μακρόχρονες και, σε συχνές περιπτώσεις, άλυτες διαμάχες σχετικά με την τεχνική και ηθική κατεύθυνση της βάσης κώδικα.

Μπορεί και πρέπει να υποστηριχθεί ότι πολλές από αυτές τις διαφωνίες, και η κατάρρευση της κοινότητας που προκύπτει όταν αναλαμβάνεται δράση, είναι άμεσο αποτέλεσμα της έλλειψης επίσημων διαδικασιών για τη συζήτηση αλλαγής.

Πως μπορεί κανείς να πείσει τους χρήστες Bitcoin να υιοθετήσουν το Segregated Witness; Πώς πρέπει οι βασικοί προγραμματιστές του Ethereum να μετρήσουν το συναίσθημα της κοινότητας για τη διάσωση του DAO; Εάν η κοινότητα σπάσει, τα κρυπτονομίσματα είναι κατεστραμμένα;

Στις χειρότερες περιπτώσεις, η ηθική εξουσία για να ενεργήσει θα μπορούσε απλώς να ανατεθεί σε όποιον έχει τους προγραμματιστές, τις σχέσεις υποδομής και τα χρήματα, όχι τις καλύτερες ευχές της συντριπτικής πλειονότητας της κοινότητας. Επιπλέον, εάν ένα μεγάλο μέρος της κοινότητας είναι απρόσιτο ή απεμπλακεί λόγω κακών κινήτρων, τότε πώς μπορεί κανείς πραγματικά να γνωρίζει εάν οι πράξεις του είναι νόμιμες;

Τα προτεινόμενα κρυπτονομίσματα όπως το Tezos παρέχουν ένα ενδιαφέρον μοντέλο για να εξετάσουμε πού αντιμετωπίζεται ένα πρωτόκολλο κρυπτογράφησης σαν ένα σύνταγμα που περιέχει τρεις ενότητες (Συναλλαγή, συναίνεση και δίκτυο) με ένα σύνολο τυπικών κανόνων και διαδικασίας για την ενημέρωση του συντάγματος. Ωστόσο, μένει να γίνει πολλή δουλειά με κίνητρα και για το πώς ακριβώς να μοντελοποιηθεί και να αλλάξει ένα κρυπτογράφηση με μια επίσημη γλώσσα.

Η χρήση τυπικών μεθόδων, οι κατανοητές από τον υπολογιστή προδιαγραφές και η συγχώνευση ενός ταμείου με αυτήν τη διαδικασία για οικονομικά κίνητρα διερευνώνται ως πιθανές δυνατότητες έμπνευσης. Τελικά, μόνο η δυνατότητα πρότασης αλλαγής πρωτοκόλλου με διαφανή τρόπο χωρίς λογοκρισία με ψηφοφορία βάσει blockchain θα βελτιώσει τη διαδικασία, ακόμη και αν δεν μπορούν να σχεδιαστούν πιο κομψές λύσεις.

Σχεδιασμός σε επίπεδα – Cardano Settlement Layer

Όταν σχεδιάζετε υπέροχα πρωτόκολλα και γλώσσες, δεν πρέπει να κοιτάτε το μέλλον, αλλά το παρελθόν. Η ιστορία παρέχει μια σειρά από παραδείγματα εξαιρετικών ιδεών που είναι τέλεια σε χαρτί, αλλά κατά κάποιον τρόπο δεν έχουν επιβιώσει, όπως τα πρότυπα Open Systems Interconnection. Η ιστορία παρέχει επίσης ευτυχή ατυχήματα που έχουν υποστεί από TCP / IP έως JavaScript.

Ορισμένες αρχές που εξάγονται από μια ιστορική άποψη είναι οι ακόλουθες:

1. Δεν μπορείτε να προβλέψετε το μέλλον, οπότε χτίστε το κάθε δωμάτιο πρώτα.
2. Η πολυπλοκότητα είναι ωραία σε χαρτί, αλλά η απλότητα κερδίζει συνήθως.
3. Όπου λαλούν πολλοί κοκκόροι αργεί να ξημερώσει.
4. Μόλις οριστεί ένα πρότυπο, πιθανότατα θα παραμείνει, ανεξάρτητα από το αν δεν είναι το βέλτιστο.
5. Οι κακές ιδέες μπορούν πραγματικά να εξελιχθούν σε πολύ καλές, εάν υπάρχει θέληση

Το Cardano είναι ένα χρηματοοικονομικό σύστημα που αποδέχεται την κοινωνική του φύση. Θα υπάρχει τεράστια ανάγκη για ευελιξία και ικανότητα αντιμετώπισης της αυθαίρετης πολυπλοκότητας στη συναλλαγή ενός συγκεκριμένου χρήστη. Εάν είναι επιτυχής, θα υπάρχει ανάγκη για τεράστιους υπολογιστικούς πόρους, αποθηκευτικούς και δικτυακούς πόρους για την εξυπηρέτηση εκατομμυρίων ταυτόχρονων συναλλαγών.

Ωστόσο, δεν διαθέτουμε έναν ψηφιακό, αποκεντρωμένο "Ρομπέν των Δασών" που θα πάρει από τους πλούσιους κόμβους και να τους δώσουμε στους φτωχούς για να επιτύχουμε ένα δίκαιο δίκτυο. Ούτε έχουμε την πολυτέλεια να εμπιστευόμαστε την ανθρώπινη ευεργεσία για να θυσιάστουμε αλτρουιστικά για το μεγαλύτερο καλό του δικτύου. Επομένως, ο σχεδιασμός της Cardano δανείζεται από το TCP/IP την έννοια του διαχωρισμού των ανησυχιών

Τα Blockchains είναι τελικά βάσεις δεδομένων που ταξινομούν γεγονότα και συμβάντα με εγγυήσεις σχετικά με τις χρονικές σφραγίδες και το αμετάβλητο. Στο πλαίσιο των χρημάτων, διατάζουν την κυριότητα των περιουσιακών στοιχείων. Η προσθήκη πολύπλοκων υπολογισμών με αποθήκευση και εκτέλεση προγραμμάτων είναι μια ορθολογική ιδέα. Θέλουμε να μάθουμε πόση αξία πήγε από την Αλίκη στον Μπομπ ή θέλουμε να ασχοληθούμε με το να καταλάβουμε ολόκληρη την ιστορία πίσω από τη συναλλαγή και να αποφασίσουμε πόσο θα στείλουμε;

Είναι απίστευτα δελεαστικό να επιλέξουμε το τελευταίο όπως έκανε το Ethereum επειδή είναι πιο ευέλικτο, αλλά παραβιάζει τις αρχές σχεδιασμού παραπάνω. Η καταγραφή της ιστορίας σημαίνει ότι ένα μόνο πρωτόκολλο πρέπει να είναι σε θέση να κατανοεί τα αυθαίρετα γεγονότα, τις αυθαίρετες συναλλαγές σεναρίων, να επιτρέπει τη διαιτησία σε περιπτώσεις απάτης και ακόμη και ενδεχομένως να αντιστρέφει τις συναλλαγές όταν διατίθενται νέες πληροφορίες.

Στη συνέχεια, πρέπει κανείς να πάρει δύσκολες αποφάσεις σχεδιασμού σχετικά με τα μεταδεδομένα που θα αποθηκεύονται για κάθε συναλλαγή. Ποια στοιχεία της ιστορίας πίσω από τη συναλλαγή της Άλις και του Μπομπ είναι σχετικά; Είναι συναφή για πάντα; Πότε μπορούμε να απορρίψουμε ορισμένα δεδομένα; Κάτι τέτοιο παραβιάζει το νόμο σε ορισμένες χώρες;

Επιπλέον, ορισμένοι υπολογισμοί έχουν ιδιωτικό χαρακτήρα. Για παράδειγμα, κατά τον υπολογισμό του μέσου μισθού των εργαζομένων σε ένα γραφείο, δεν θα θέλαμε απαραίτητα να διαρρεύσουμε πόσα χρήματα παίρνει κάθε άτομο. Τι γίνεται όμως αν κάθε υπολογισμός είναι γνωστός στο κοινό; Τι γίνεται αν αυτή η δημοσιότητα προκαλεί προκατάληψη εκτέλεσης για να βλάψει το αποτέλεσμα;

Έτσι, έχουμε επιλέξει τη θέση ότι η λογιστική της αξίας πρέπει να διαχωριστεί από την ιστορία πίσω από το γιατί μετακινήθηκε η αξία. Με άλλα λόγια, ο διαχωρισμός της αξίας από τον υπολογισμό. Αυτός ο

διαχωρισμός δεν σημαίνει ότι η Cardano δεν θα υποστηρίζει έξυπνα συμβόλαια. Αντιθέτως, καθιστώντας το διαχωρισμό σαφές, επιτρέπει σημαντικά μεγαλύτερη ευελιξία στο σχεδιασμό, τη χρήση, το απόρρητο και την εκτέλεση έξυπνων συμβάσεων.

Το καθολικό τιμής ονομάζεται Cardano Settlement Layer (CSL). Καθώς ο σκοπός είναι να ληφθεί υπόψη η αξία, ο χάρτης πορείας ("roadmap") έχει τους ακόλουθους στόχους:

1. Να υποστηρίξει δύο σειρές γλωσσών, μιας για να μετακινήσει την τιμή και ένα άλλο για να βελτιώσει την υποστήριξη πρωτοκόλλου επικάλυψης.
2. Να παρέχει υποστήριξη για τις πλευρικές αλυσίδες KMZ5 για σύνδεση με άλλα καθολικά.
3. Να υποστηρίξει πολλαπλούς τύπους υπογραφών, συμπεριλαμβανομένων κβαντικών ανθεκτικών υπογραφών για μεγαλύτερη ασφάλεια.
4. Να υποστηρίξει πολλαπλά στοιχεία που εκδόθηκαν από τον χρήστη.
5. Να αποκτήσει πραγματική δυνατότητα κλιμάκωσης, που σημαίνει καθώς όλο και περισσότεροι χρήστες συμμετέχουν, οι δυνατότητες του συστήματος θα αυξάνονται.

Συγγραφή σεναρίου ("scripting")

Ξεκινώντας με τη γλώσσα γραφής, οι συναλλαγές μεταξύ διευθύνσεων σε ένα καθολικό απαιτούν κάποια μορφή σεναρίου για να εκτελεστούν και να αποδειχθούν έγκυρες. Στην ιδανική περίπτωση, κάποιος δεν θα ήθελε η Εύα να αποκτήσει πρόσβαση στα χρήματα της Αλίκης, ούτε κανείς θα ήθελε κάποιο κακό σενάριο να στείλει κατά λάθος αξία σε μια νεκρή ("dead") διεύθυνση κάνοντας τα χρήματα ανεπανόρθωτα.

Συστήματα όπως το Bitcoin παρέχουν μια εξαιρετικά άκαμπτη και δρακόντια γλώσσα σεναρίων που είναι δύσκολο να προγραμματιστούν κατά παραγγελία συναλλαγές και να διαβαστούν και να κατανοηθούν. Ωστόσο, η γενική δυνατότητα προγραμματισμού γλωσσών, όπως η Solidity, εισάγει μια εξαιρετική πολυπλοκότητα στο σύστημα και είναι χρήσιμη σε ένα πολύ μικρότερο σύνολο παραγόντων.

Ως εκ τούτου, επιλέξαμε να σχεδιάσουμε μια νέα γλώσσα που ονομάζεται Simon προς τιμήν του δημιουργού της Simon Thompson και του δημιουργού των εννοιών που την ενέπνευσαν, Simon Peyton Jones. Η Simon είναι μια γλώσσα για συγκεκριμένο τομέα που βασίζεται στη σύνθεση συμβολαίων: μια περιπέτεια στον τομέα της χρηματοοικονομικής μηχανικής.

Η βασική ιδέα είναι ότι οι χρηματοοικονομικές συναλλαγές αποτελούνται γενικά από μια συλλογή θεμελιωδών στοιχείων. Εάν κάποιος συγκεντρώσει έναν οικονομικό περιοδικό πίνακα στοιχείων, τότε μπορεί να παρέχει υποστήριξη για ένα αυθαίρετα μεγάλο σύνολο σύνθετων συναλλαγών που θα καλύπτει τους περισσότερους, αν όχι όλους, κοινούς τύπους συναλλαγών χωρίς να απαιτείται γενικά προγραμματισμός.

Το πρωταρχικό πλεονέκτημα είναι ότι η ασφάλεια και η εκτέλεση μπορεί να γίνει πολύ καλά κατανοητή. Μπορούν να γραφτούν αποδείξεις για να δείξουν την ορθότητα των προτύπων και να εξαντλήσουν τον χώρο εκτέλεσης των προβληματικών συμβάντων συναλλαγών, όπως η δημιουργία νέου χρήματος από

τον αέρα ή την ευελιξία συναλλαγών. Δεύτερον, μπορεί κανείς να αφήσει σε επεκτάσεις για να προσθέσει περισσότερα στοιχεία μέσω μαλακών πιρουνιών, εάν απαιτείται νέα λειτουργικότητα.

Αφού είπαμε αυτό, θα υπάρχει πάντα ανάγκη σύνδεσης CSL σε πρωτόκολλα επικάλυψης, χρηματοοικονομικά συστήματα παλαιού τύπου και διακομιστές ειδικού σκοπού. Έτσι, έχουμε αναπτύξει το Plutus ως γλώσσα έξυπνης σύμβασης γενικής χρήσης και ως DSL ειδικού σκοπού για διαλειτουργικότητα.

Το Plutus είναι μια δακτυλογραφημένη λειτουργική γλώσσα που βασίζεται σε έννοιες από τη Haskell, η οποία μπορεί να χρησιμοποιηθεί για τη σύνταξη προσαρμοσμένων σεναρίων συναλλαγών. Για το CSL, θα χρησιμοποιηθεί για σύνθετες συναλλαγές που απαιτούνται για την προσθήκη υποστήριξης για άλλα επίπεδα που πρέπει να συνδεθούμε, όπως το πρόγραμμα μας στα sidechains.

Sidechains

Όσον αφορά τα sidechains, η Cardano θα υποστηρίξει ένα νέο πρωτόκολλο που αναπτύχθηκε από τους Kiayias, Miller και Zindros (KMZ sidechains) με βάση προηγούμενα αποτελέσματα από αποδείξεις απόδειξης (“proof of proof”) εργασίας. Ο συγκεκριμένος σχεδιασμός είναι εκτός του πεδίου αυτού του εγγράφου. Ωστόσο, η ιδέα επιτρέπει την ασφαλή και μη διαδραστική μεταφορά χρημάτων από το CSL σε οποιοδήποτε Cardano Computation Layer ή άλλο blockchain που υποστηρίζει το πρωτόκολλο.

Τα sidechains KMZ είναι το κλειδί για την πολυπλοκότητα ενθυλάκωσης (“encapsulating”). Τα καθολικά με τις κανονιστικές απαιτήσεις, τις ιδιωτικές λειτουργίες, τις ισχυρές γλώσσες δέσμης ενεργειών και άλλες ειδικές ανησυχίες είναι ουσιαστικά μαύρα κουτιά στο CSL, ωστόσο ο χρήστης του CSL θα αποκτήσει ορισμένες εγγυήσεις σχετικά με τη λογιστική και την ικανότητα ανάκλησης χρημάτων μόλις ολοκληρωθεί ο υπολογισμός

Επιστήμη και Μηχανική

Η τέχνη της επανάληψης

Τα κρυπτονομίσματα είναι πρωτόκολλα που εφαρμόζονται ως λογισμικό. Τα πρωτόκολλα είναι απλώς έξυπνες συνομιλίες μεταξύ των συμμετεχόντων. Το λογισμικό είναι τελικά ο χειρισμός των δεδομένων, δεδομένου κάποιου στόχου. Ωστόσο, η διαφορά μεταξύ στερεού, αξιόπιστου λογισμικού, καθώς και χρήσιμων, ασφαλών πρωτοκόλλων και του αντίστροφου είναι εντελώς ανθρώπινη.

Το καλό λογισμικό χρειάζεται λογοδοσία, σαφείς επιχειρηματικές απαιτήσεις, επαναλαμβανόμενες διαδικασίες, διεξοδικές δοκιμές και ακούραστη επανάληψη. Το καλό λογισμικό χρειάζεται επίσης αρκετούς ταλαντούχους προγραμματιστές με αρκετή γνώση συγκεκριμένου τομέα για να σχεδιάσει σωστά ένα σύστημα που μπορεί να επιλύσει πλήρως οποιοδήποτε πρόβλημα προσπαθούν να λύσουν.

Όσον αφορά τα χρήσιμα και ασφαλή πρωτόκολλα, ειδικά εκείνα που περιλαμβάνουν κρυπτογραφία και κατανεμημένα συστήματα, ξεκινούν με μια πιο ακαδημαϊκή και βασισμένη σε πρότυπα διαδικασία. Η αξιολόγηση από ομοτίμους, ατελείωτες συζητήσεις και μια σταθερή έννοια των συμβιβασμών είναι απαραίτητες για να διασφαλιστεί ότι ένα πρωτόκολλο είναι χρήσιμο. Ωστόσο, αυτά από μόνα τους δεν επαρκούν, τα πρωτόκολλα πρέπει να εφαρμοστούν και να δοκιμαστούν από την πραγματική χρήση.

Η μοναδική πρόκληση στη βιομηχανία κρυπτονομισμάτων είναι ότι δύο εντελώς διαφορετικές φιλοσοφίες συγχωνεύονται χωρίς μια σωστή Hegelian σύνθεση. Η διατριβή μας είναι μια νοοτροπία εκκίνησης «γρήγορης κίνησης και σπασίματος πραγμάτων» με γνώμονα τη νεολαία, την απληστία και το πάθος. Η αντίθεση είναι μια αργή, μεθοδική και ακαδημαϊκά προσανατολισμένη προσέγγιση, η οποία υποκινείται από την επιθυμία να παγιώσει τις καινοτομίες του χώρου μας σε μια ωραία θέση απολαμβάνοντας άφθονη χρηματοδότηση και κύρος.

Το αποτέλεσμα είναι ότι πολλά κρυπτονομίσματα είτε ορίζονται εξ ολοκλήρου σε ένα whitepaper που σχετίζονται μόνο με ένα βιογραφικό σημείωμα είτε απλά με έναν βιαστικά γραμμένο κώδικα. Κανένα από τα τρέχοντα κορυφαία δέκα κρυπτονομίσματα σε κεφαλαιοποίηση της αγοράς δεν βασίζεται σε ένα πρωτόκολλο αξιολόγησης από ομοτίμους. Κανένα από τα δέκα κορυφαία κρυπτονομίσματα δεν εφαρμόστηκε από επίσημες προδιαγραφές.

Ωστόσο, διακυβεύονται δισεκατομμύρια δολάρια αξίας. Μόλις αναπτυχθεί, ένα κρυπτονόμισμα είναι εξαιρετικά δύσκολο να αλλάξει. Πώς γνωρίζει ο χρήστης ότι χρησιμοποιεί ένα ασφαλές σύστημα; Πώς γνωρίζει ο χρήστης ότι οι ισχυρισμοί μάρκετινγκ είναι νόμιμοι; Τι γίνεται αν το προτεινόμενο πρωτόκολλο δεν μπορεί ποτέ να επιτύχει τους ισχυρισμούς;

Αυτή η έλλειψη σύνθεσης και σεβασμού στη διαδικασία είναι ένας από τους κύριους λόγους που η IOHK ήθελε να χτίσει το Cardano. Η ελπίδα μας ήταν να αναπτύξουμε ένα έργο αναφοράς που θα χρησιμεύσει ως παράδειγμα του πώς να κάνουμε τα πράγματα με πιο αποτελεσματικό, λογικό και τίμιο τρόπο.

Ο στόχος δεν είναι να προτείνουμε έναν εντελώς νέο τρόπο ανάπτυξης λογισμικού και πρωτοκόλλων, αλλά μάλλον να αναγνωρίσουμε ότι υπάρχει ήδη μεγάλο λογισμικό και πρωτόκολλα και μπορούμε να μιμηθούμε τις συνθήκες που οδήγησαν στη δημιουργία τους. Δεύτερον, να γίνουν γνωστές και ανοιχτές πηγές αυτές οι συνθήκες, εάν είναι δυνατόν, ώστε να μπορούν να μιμηθούν προς όφελος ολόκληρου του πεδίου.

Γεγονότα και Γνώμες

Η άλλη ανησυχία είναι για το πού τελειώνουν τα γεγονότα και αρχίζει η γνώμη. Υπάρχουν εκατοντάδες γλώσσες προγραμματισμού, δεκάδες παραδείγματα ανάπτυξης και περισσότερες από μία φιλοσοφίες στη διαχείριση έργων. Ο ακαδημαϊκός κόσμος γεμίζει τις δικές του προκλήσεις που απορρέουν από την απόστασή του από επιχειρηματικές ανησυχίες και πρακτικότητα.

Για το Cardano, προσπαθήσαμε πρώτα να καταγράψουμε προφανείς ελλείψεις που μπορούν να συμφωνηθούν παγκοσμίως ως χρήσιμες από την άποψη της μηχανικής. Για παράδειγμα, η

κρυπτογραφία και τα κατανεμημένα συστήματα είναι και τα δύο εξαιρετικά ασυνήθιστα θέματα με πάρα πολλά παραδείγματα για το πώς τα αφελείς χέρια μπορούν να κάνουν τρομερά λάθη. Επομένως, κάθε πρωτόκολλο που απαιτεί πληροφορίες από αυτούς τους τομείς πρέπει να σχεδιαστεί από έναν αναγνωρισμένο εμπειρογνώμονα και να υποβληθεί για έλεγχο από άλλους εμπειρογνώμονες.

Το Ouroboros είναι η πρώτη μας μελέτη περίπτωσης ("case study") αυτής της περιοχής. Σχεδιάστηκε από μια ομάδα κρυπτογράφων με μεγάλο, ποικίλο και δημοσίως επαληθεύσιμο ιστορικό δημοσίευσης. Κατασκευάστηκε σύμφωνα με την τυπική διαδικασία κρυπτογράφησης, με παραδοχές ασφάλειας και αποδείξεις. Αυτές οι αποδείξεις ελέγχθηκαν με υποβολή σε συνέδρια και επίσης ανεξάρτητα από αποδείξεις μέσω υπολογιστή που γράφτηκαν στην Isabelle από μια ομάδα στο Πανεπιστήμιο του Cambridge.

Ωστόσο, αυτή η εργασία από μόνη της δεν παρέχει εγγυήσεις χρησιμότητας - μόνο έναν αυστηρό έλεγχο ενός μοντέλου ασφαλείας, λαμβάνοντας υπόψη ορισμένες υποθέσεις. Για χρησιμότητα, πρέπει να εφαρμοστεί και να δοκιμαστεί το πρωτόκολλο. Οι προγραμματιστές μας το έχουν κάνει τόσο στο Haskell όσο και στο Rust. Αυτό το έργο αποκάλυψε ότι χρειάζεται περισσότερη προσπάθεια να επικεντρωθεί στο μοντέλο συγχρονισμού, το οποίο οδήγησε στη δημιουργία του Ouroboros Praos.

Αυτή η τέχνη της επανάληψης είναι αυτό που παράγει εξαιρετικά πρωτόκολλα, με κάθε βήμα να οδηγεί σε νέα μαθήματα και μια απαίτηση να επαληθεύσει εκ νέου την ορθότητα του προηγούμενου βήματος. Είναι δαπανηρό, χρονοβόρο και μερικές φορές πραγματικά κουραστικό, ωστόσο απαιτείται να διασφαλιστεί ότι το πρωτόκολλο έχει σχεδιαστεί σωστά.

Τα πρωτόκολλα - ειδικά αυτά που χρησιμοποιούνται από δισεκατομμύρια άτομα - δεν είναι βραχύβια και εξελίσσονται γρήγορα. Αντίθετα, πρέπει να ακολουθούνται για χρόνια έως δεκαετίες. Φαίνεται απολύτως λογικό ότι, προτού επιβαρύνουμε τον κόσμο με ένα νέο χρηματοπιστωτικό σύστημα που όλοι πρέπει να ζήσουμε για τα επόμενα 100 χρόνια, θέλουμε να απαιτήσουμε λίγο περιθώριο και αυστηρότητα από τους σχεδιαστές του

Λειτουργικές Αμαρτίες

Μεταβαίνοντας σε μια περιοχή με περισσότερες απόψεις, τα εργαλεία, οι γλώσσες και οι μεθοδολογίες που χρησιμοποιούνται στην ανάπτυξη λογισμικού είναι περισσότερο αντικείμενα θρησκευτικής φροντίδας παρά αντικειμενικής πραγματικότητας. Ο πηγαίος κώδικας είναι σαν γραπτή πεζογραφία. Ο καθένας έχει τη γνώμη για το τι είναι καλό - και αυτό που κοινοποιείται είναι, μερικές φορές, λιγότερο σημαντικό από το πώς μεταδίδεται.

Πρέπει να διαπράξουμε την αμαρτία να επιλέξουμε μια πλευρά που να αποδέχεται ότι θα είναι λάθος τουλάχιστον στα μάτια ενός ατόμου. Ωστόσο, υπάρχει τουλάχιστον ένα μεγάλο εύρος δικαιολογίας πίσω από την επιλογή μας.

Τα πρωτόκολλα που καθιστούν δυνατό το Cardano εφαρμόζονται στο Haskell. Το προφίλ χρήστη ("user interface") έχει ενσωματωθεί σε ένα πιρούνι του Electron που ονομάζουμε Daedalus. Επιλέξαμε να

χρησιμοποιήσουμε το αρχιτεκτονικό μοντέλο ιστού όπου είναι δυνατόν, και για τη βάση δεδομένων μας, επιλέξαμε ένα παράδειγμα κλειδιού-τιμής χρησιμοποιώντας το RocksDB.

Σε επίπεδο συστατικού, αυτή η αφαίρεση σημαίνει ότι η συντήρηση είναι πολύ απλούστερη, η καλύτερη τεχνολογία μπορεί να αντικατασταθεί αργότερα με λίγη προσπάθεια και ότι η στοίβα μας συνδέεται εν μέρει με τις προσπάθειες ανάπτυξης του Github και του Facebook.

Η χρήση ενός WebGuI μας επιτρέπει να αξιοποιήσουμε το React και να αναπτύξουμε λειτουργίες διεπαφής χρησιμοποιώντας εργαλεία που είναι κατανοητά από εκατοντάδες χιλιάδες προγραμματιστές JavaScript. Η χρήση αρχιτεκτονικής ιστού σημαίνει ότι τα στοιχεία μπορούν να θεωρηθούν υπηρεσίες και το μοντέλο ασφαλείας είναι λογικό.

Η επιλογή του Haskell για ανάπτυξη πρωτοκόλλου ήταν η πιο δύσκολη επιλογή. Ακόμα και στον λειτουργικό κόσμο, υπάρχουν πολλές επιλογές. Από την πιο ευέλικτη και ακάθαρτη πλευρά, υπάρχουν γλώσσες όπως το Clojure, το Scala και το F #, που επωφελούνται από τις τεράστιες βιβλιοθήκες της Java και των .Net οικοσυστημάτων, διατηρώντας παράλληλα μερικές από τις καλύτερες πτυχές του λειτουργικού προγραμματισμού.

Υπάρχουν περισσότερες ακαδημαϊκά προσανατολισμένες γλώσσες όπως η Agda και η Idris που έχουν στενή σύνδεση με τεχνικές που θα επέτρεπαν την ισχυρή επαλήθευση της ορθότητας. Ωστόσο, στερούνται λογικών βιβλιοθηκών και έχουν μια ανώτερη εμπειρία ανάπτυξης.

Για τον Cardano, η επιλογή ήρθε σε Ocaml και Haskell. Η Ocaml είναι μια υπέροχη γλώσσα με μια υπέροχη κοινότητα, καλά εργαλεία, λογική εμπειρία ανάπτυξης και εξαιρετική κληρονομιά στον επίσημο χώρο επαλήθευσης μέσω του Coq. Γιατί λοιπόν επιλέξαμε τη Haskell;

Γιατί Haskell?

Τα πρωτόκολλα που συνθέτουν το Cardano διανέμονται, ομαδοποιούνται με κρυπτογραφία και απαιτούν υψηλό βαθμό ανοχής σφαλμάτων. Τις καλύτερες μέρες, θα εξακολουθούν να υπάρχουν βυζαντινοί ηθοποιοί, μηνύματα με λανθασμένη μορφή και ελαττωματικοί πελάτες που προκαλούν ακούσια κάποια καταστροφή στο δίκτυο.

Πρώτον, θέλαμε μια γλώσσα που να διαθέτει ένα ισχυρό σύστημα τύπου όπου θα μπορούσαμε εύκολα να χρησιμοποιήσουμε εργαλεία όπως το Quickcheck και πιο περίπλοκες τεχνικές όπως οι Τύποι βελτίωσης, ενώ έχουμε μια λογική προσδοκία για ανοχή σφαλμάτων. Ένα μοντέλο OTP τύπου Erlang ικανοποιεί το δεύτερο, ενώ γλώσσες όπως οι Haskell και Ocaml ικανοποιούν το πρώτο.

Με την εισαγωγή του Cloud Haskell, ο Haskell απέκτησε πολλά από τα πλεονεκτήματα της Erlang χωρίς να παραδώσει τα δικά του. Επιπλέον, η αρθρωτότητα και η συνθεσιμότητα του Haskell μας επέτρεψαν

να χρησιμοποιήσουμε μια βιβλιοθήκη κατά παραγγελία με μικρότερο βάρος που ονομάζεται Time Warp for Cardano.

Δεύτερον, οι βιβλιοθήκες της Haskell έχουν εξελιχθεί πολύ τα τελευταία χρόνια χάρη στο εκτεταμένο έργο εμπορικών οντοτήτων όπως το Galois, το FP Complete και το Well-Typed. Κατά συνέπεια, η Haskell μπορεί να χρησιμοποιηθεί για τη σύνταξη εφαρμογών παραγωγής.

Τρίτον, η ταχεία εξέλιξη του PureScript παρείχε μια πολύ απαραίτητη γέφυρα στον κόσμο της JavaScript παρόμοια με αυτό που έδωσε το Clojurescript στο Clojure. Αναμένουμε ότι το PureScript θα είναι ιδιαίτερα σημαντικό όταν πρόκειται για το Cardano να δουλέψει σε ένα πρόγραμμα περιήγησης και να αναπτύξει πορτοφόλια για κινητά.

Τέταρτον, όσον αφορά την επίλυση εξάρτησης, η Haskell τα τελευταία χρόνια έχει απολαύσει μια σημαντική κοινωνική και τεχνολογική προσπάθεια με επικεφαλής τεχνολόγους όπως ο Michael Snoyman μέσω μιας πλατφόρμας που ονομάζεται stackage, η οποία είναι εύκολη στη χρήση και υποστηρίζεται καλά από το FP Complete.

Πέμπτον, πέρα από την επαρκή ανάλυση εξάρτησης, στοχεύουμε η αναπαραγωγή του λογισμικού μας. Με άλλα λόγια, με τις ίδιες τιμές διαμόρφωσης και εκδόσεις εξάρτησης θα πρέπει να παράγει ακριβώς τα ίδια αντικείμενα κατασκευής. Μέσω του stackage, χρησιμοποιούμε το NixOps για να επιτύχουμε την αναπαραγωγιμότητα με μεγάλη επιτυχία.

Τέλος, το ταλέντο των προγραμματιστών που ειδικεύονται στη Haskell είναι αρκετά μεγάλο - σε σύγκριση με τους συναδέλφους τους - και αρκετά καλά εκπαιδευμένο με το σωστό συνδυασμό ακαδημαϊκών και βιομηχανικών διαπιστευτηρίων. Λειτουργεί επίσης ως φίλτρο ικανότητας, καθώς είναι ασυνήθιστο να βρίσκετε έμπειρους προγραμματιστές Haskell χωρίς λεπτομερείς γνώσεις σχετικά με την επιστήμη των υπολογιστών.

Τυπικές προδιαγραφές και επαλήθευση

Ένα σημαντικό πλεονέκτημα της ανάπτυξης ενός πρωτοκόλλου χρησιμοποιώντας ένα αποδεδειγμένα σωστό μοντέλο ασφάλειας είναι ότι παρέχει ένα εγγυημένο όριο “αντιπαλότητας”. Σε έναν έχει δοθεί ένα συμβόλαιο ότι όσο ακολουθεί το πρωτόκολλο και οι αποδείξεις είναι σωστές, ο “αντίπαλος” δεν μπορεί να παραβιάσει τις αξίες ασφαλείας που αξιώνονται.

Ο βαθύτερος προβληματισμός καθιστά τον προηγούμενο ισχυρισμό ακόμη πιο σημαντικό. Οι “αντίπαλοι” μπορούν να είναι αυθαίρετα έξυπνοι και ικανοί. Το να λέμε ότι νικήθηκαν μόνο μέσω ενός μαθηματικού μοντέλου είναι εξαιρετικό. Και, φυσικά, δεν είναι απολύτως αλήθεια.

Η πραγματικότητα εισάγει παράγοντες και περιστάσεις που εμποδίζουν την ουτοπία της καθαρής ασφάλειας και της σωστής συμπεριφοράς από την ύπαρξη. Οι υλοποιήσεις μπορεί να είναι λανθασμένες. Το υλικό μπορεί να εισαγάγει διανύσματα επίθεσης που προηγουμένως δεν είχαν ληφθεί υπόψη. Το μοντέλο ασφαλείας μπορεί να είναι ανεπαρκές και να μην συμμορφώνεται με την πραγματική χρήση.

Απαιτείται κρίση σχετικά με το πόσο απαιτούνται προδιαγραφές, αυστηρότητα και έλεγχος για ένα πρωτόκολλο. Για παράδειγμα, προσπάθειες όπως το έργο SeL4 Microkernel είναι ένα πρωταρχικό παράδειγμα μιας εξ ολοκλήρου επίθεσης στην ασάφεια που απαιτεί σχεδόν 200.000 γραμμές κώδικα Isabelle για την επαλήθευση λιγότερων από 10.000 γραμμών κώδικα C. Ωστόσο, ο πυρήνας του λειτουργικού συστήματος είναι κρίσιμη υποδομή που θα μπορούσε να είναι μια σοβαρή ευπάθεια ασφαλείας, εάν δεν εφαρμοστεί σωστά.

Πρέπει όλα τα κρυπτογραφικά λογισμικά να απαιτούν την ίδια ηράκλεια προσπάθεια; Ή μπορεί κανείς να επιλέξει ένα λιγότερο έντονο μονοπάτι που παράγει ισοδύναμα αποτελέσματα; Επίσης, έχει σημασία εάν το πρωτόκολλο εφαρμόζεται τέλεια εάν το περιβάλλον στο οποίο είναι γνωστό είναι ευάλωτο όπως στα Windows XP;

Για το Cardano, επιλέξαμε τον ακόλουθο συμβιβασμό. Πρώτον, λόγω της πολύπλοκης φύσης των τομέων της κρυπτογραφίας και του κατανεμημένου υπολογισμού, οι αποδείξεις τείνουν να είναι πολύ λεπτές, μακρές, περίπλοκες και μερικές φορές αρκετά τεχνικές. Αυτό σημαίνει ότι ο έλεγχος από τον άνθρωπο μπορεί να είναι κουραστικός και επιρρεπής σε σφάλματα. Επομένως, πιστεύουμε ότι κάθε σημαντική απόδειξη που παρουσιάζεται σε ένα whitepaper γραμμένο για την κάλυψη των βασικών υποδομών, πρέπει να ελεγχθεί μηχανικά.

Δεύτερον, για να επαληθεύσουμε τον κωδικό Haskell έτσι ώστε να αντιστοιχεί σωστά στα whitepapers μας, μπορούμε να επιλέξουμε μεταξύ δύο δημοφιλών επιλογών: διασύνδεση με SMT provers μέσω LiquidHaskell και χρήση Isabelle / HOL.

Οι λύσεις SMT (satisfiability modulo θεωρίες) αντιμετωπίζουν το πρόβλημα της εύρεσης λειτουργικών παραμέτρων που ικανοποιούν μια εξίσωση ή ανισότητα, ή εναλλακτικά δείχνοντας ότι τέτοιες παράμετροι δεν υπάρχουν. Όπως συζητήθηκε από τους De Moura και Bjørner, οι περιπτώσεις χρήσης του SMT είναι διάφορες, αλλά το βασικό σημείο είναι ότι αυτές οι τεχνικές είναι και οι δύο ισχυρές και μπορούν να μειώσουν δραματικά τα σφάλματα και τα σημασιολογικά λάθη.

Το Isabelle / HOL, από την άλλη πλευρά, είναι ένα πιο εκφραστικό και ποικίλο εργαλείο που μπορεί να χρησιμοποιηθεί τόσο για τον καθορισμό όσο και για την επαλήθευση της εφαρμογής. Το Isabelle είναι ένα γενικό θεώρημα επίλυσης που λειτουργεί με δομές λογικής υψηλότερης τάξης, ικανό να αντιπροσωπεύει σύνολα και άλλα μαθηματικά αντικείμενα που θα χρησιμοποιηθούν σε αποδείξεις. Η ίδια η Isabelle ενσωματώνεται με τον Z3 SMT prover για την αντιμετώπιση προβλημάτων που συνεπάγονται τέτοιους περιορισμούς.

Και οι δύο προσεγγίσεις παρέχουν αξία και ως εκ τούτου αποφασίσαμε να τις αγκαλιάσουμε και τις δύο σταδιακά. Ανθρώπινα γραπτά αποδεικτικά στοιχεία θα κωδικοποιηθούν στο Isabelle για να ελέγξουν την ορθότητά τους, ικανοποιώντας έτσι την απαίτηση ελέγχου μηχανήματος. Και σκοπεύουμε να προσθέσουμε σταδιακά το Liquid Haskell σε όλους τους κωδικούς παραγωγής στην εφαρμογή του Cardano κατά τη διάρκεια του 2017 και του 2018.

Ως τελικό σημείο, η επίσημη επαλήθευση είναι τόσο καλή όσο η προδιαγραφή επαληθεύει και τα διαθέσιμα εργαλεία. Ένας από τους κύριους λόγους για την επιλογή του Haskell είναι ότι παρέχει τη

σωστή ισορροπία πρακτικότητας και θεωρίας. Η προδιαγραφή που προέρχεται από τη Λευκή Βίβλο μοιάζει πολύ με τον κωδικό Haskell και η σύνδεση των δύο είναι πολύ πιο εύκολη από το να το κάνει με μια επιτακτική γλώσσα.

Υπάρχει ακόμη τεράστια δυσκολία στην καταγραφή μιας σωστής προδιαγραφής και επίσης ενημέρωση της προδιαγραφής όταν πρέπει να γίνουν αλλαγές όπως αναβαθμίσεις, διορθώσεις σφαλμάτων και άλλες ανησυχίες. Ωστόσο, αυτή η πραγματικότητα δεν μειώνει με κανέναν τρόπο τη συνολική αξία. Αν κάποιος δυσκολεύεται να οικοδομήσει ένα θεμέλιο με αποδεδειγμένη ασφάλεια, τότε η εφαρμογή θα πρέπει να είναι αυτό που πραγματικά προτάθηκε στο χαρτί.

Διαφάνεια

Μια τελευταία ερώτηση κατά τη συζήτηση της επιστήμης και της μηχανικής της ανάπτυξης κρυπτονομισμάτων είναι πώς να αντιμετωπίσετε τη διαφάνεια. Οι σχεδιαστικές αποφάσεις δεν έρχονται στους προγραμματιστές στα όνειρα τους και στη συνέχεια ξαφνικά γίνονται κανόνι. Προέρχονται από εμπειρία, συζήτηση και διδάγματα από προηγούμενα λάθη.

Η πρόκληση είναι ότι μια απόλυτα διαφανής αναπτυξιακή διαδικασία θα μπορούσε να επηρεάσει τη συζήτηση για να γίνει πιο θεατρική από ό, τι βασίζεται σε στοιχεία. Το Egos, οι απόπειρες νίκης σε μια κοινότητα και ο φόβος μήπως ακουστούν ανόητοι θα μπορούσαν να αναγκάσουν τις συνομιλίες να γίνουν στείρες και αντιπαραγωγικές.

Επιπλέον, εξωτερικοί παράγοντες θα μπορούσαν να προσπαθήσουν να εμλέξουν τη συνομιλία σε μια προσπάθεια να οδηγήσουν τη συνιστώσα τους να γίνει το μόνο σχετικό θέμα. Ο καθένας έχει μια ιερή αγελάδα.

Λοιπόν, πώς εξισορροπεί κανείς την ανάγκη για μια διαφανή αναπτυξιακή διαδικασία, η οποία οφείλεται στην κοινότητα που έχει αναθέσει την πρόοδο σε ένα σύνολο βασικών προγραμματιστών, με την ανάγκη για ελευθερία έκφρασης χωρίς φόβο;

Με το Cardano, αποφασίσαμε να ακολουθήσουμε μια τυποποιημένη διαδικασία με κατευθυνόμενη εποπτεία. Η κοινότητα πρέπει να γνωρίζει ότι η επιστήμη και ο κώδικας είναι καλά μελετημένες, ελεγμένες και πραγματικά επιλύουν τα πράγματα που ισχυρίζονται οι προγραμματιστές ότι κάνουν. Για το σκοπό αυτό, η αξιολόγηση από ομοτίμους θα πρέπει να ικανοποιεί πλήρως το επιστημονικό συστατικό, καθώς έχει σχεδιαστεί ειδικά για αυτόν τον σκοπό και μας έχει δώσει τον σύγχρονο κόσμο.

Όσον αφορά τον κώδικα, αυτό το θέμα είναι λίγο πιο διαδεδομένο. Για το Cardano, επιλέξαμε να αναθέσουμε στο Ίδρυμα Cardano να υπηρετήσει ως τελικός ελεγκτής του έργου του IOHK. Συγκεκριμένα, τους ανατίθενται οι ακόλουθες υποχρεώσεις:

1. Τακτική αναθεώρηση του πηγαίου κώδικα που περιέχεται στο Cardano Github για έλεγχο ποιότητας, δοκιμαστικής κάλυψης, κατάλληλων σχολίων και πληρότητας.
2. Επισκόπηση όλων των εγγράφων Cardano για ορθότητα και χρησιμότητα.

3. Επαλήθευση των ισχυρισμών ότι τα πρωτόκολλα που παράγονται από τους επιστήμονες εφαρμόζονται πλήρως.

Για την εκπλήρωση αυτού του έργου, η IOHK θα υποβάλλει τακτικές και έγκαιρες εκθέσεις στο Ίδρυμα - και στους εκχωρητές του - για έλεγχο. Το Ίδρυμα με τη σειρά του θα δημοσιεύσει μια έκθεση εποπτείας της ανάπτυξης στην κοινότητα Cardano τουλάχιστον σε τριμηνιαία βάση.

Αυτή η πρώτη προσπάθεια έχει ως στόχο να ξεκινήσει μια ευρύτερη συζήτηση για το πώς ένα αποκεντρωμένο έργο επιτυγχάνει λογοδοσία. Η εποπτεία της ανάπτυξης από ένα αξιόπιστο τρίτο μέρος είναι ένα ισχυρό εργαλείο για να διασφαλιστεί ότι οι προγραμματιστές βρίσκονται σε καλό δρόμο, αλλά δεν αρκεί να εγγυηθεί πλήρως ότι το έργο θα παραδίδεται πάντα.

Διαλειτουργικότητα

Η μεγάλη "μυωπία"

Η χρηματοδότηση και η ευρύτερη ιδέα του εμπορίου είναι τελικά ανθρώπινη προσπάθεια. Υπάρχουν κομψές γλώσσες, εξαιρετικά ακριβή εργαλεία για τη σύλληψη προθέσεων και ατελείωτες μάζες τεχνικών για την επίτευξη προσφυγής σε περίπτωση κακών αποτελεσμάτων, καθώς και χιλιάδων ετών νόμοι που επιδιώκουν δικαιοσύνη στο εμπόριο. Στην πραγματικότητα, μερικές από τις πρώτες μορφές γραφής ήταν εμπορικές συμβάσεις.

Ωστόσο, το ανθρώπινο στοιχείο δεν μπορεί να αποφευχθεί ανεξάρτητα από τη διαμεσολάβηση στη λογική, μηχανές ή κυβερνητικούς φρουρούς στους οποίους έχουν ανατεθεί τρομερές δυνάμεις. Εκεί βρίσκεται η μεγάλη "μυωπία" των κρυπτονομισμάτων. Είναι συνήθως διαζευγμένοι από την ανθρώπινη πραγματικότητα.

Οι άνθρωποι κάνουν λάθη. Οι άνθρωποι αλλάζουν γνώμη. Οι άνθρωποι δεν κατανοούν πάντα πλήρως τις επιχειρηματικές σχέσεις που συμφωνούν να συνάψουν. Οι άνθρωποι παραπλανούνται και εξαπατούνται. Οι περιστάσεις αλλάζουν σε ατομικό και πολιτειακό επίπεδο που απαιτούν μοναδικές λύσεις. Εξετάζοντας αυτό το σημείο, οι περισσότερες συμβάσεις περιέχουν ρήτρες ανωτέρας βίας.

Ωστόσο, τα κρυπτονομίσματα επιδιώκουν να πετάξουν την ανθρώπινη κατανόηση, συμπόνια και κρίση σε αντάλλαγμα για έναν αδιάφορο ψηφιακό δικαστή που είναι απόλυτα δεσμευμένος σε ένα σύνταγμα χωρίς να λαμβάνεται υπόψη η δικαιοσύνη ή το αποτέλεσμα. Δεδομένου ότι οι άνθρωποι πάντα προσπαθούσαν και θα συνεχίσουν να προσπαθούν να αλλάξουν κανόνες σε εγωιστικούς σκοπούς, είναι αναζωογονητικό να έχουμε ένα σύστημα που δεν μπορεί να καταστραφεί.

Αλλά τι συμβαίνει όταν ένας χρήστης πρέπει να συνδυάσει αυτά τα νέα συστήματα με παραδοσιακά χρηματοοικονομικά συστήματα; Τι συμβαίνει όταν κάποιος πρέπει να ζήσει στον ανθρώπινο κόσμο; Για παράδειγμα, τα δικαιώματα ιδιοκτησίας, όπως η εγγραφή γης, ζουν αποκλειστικά στον φυσικό κόσμο. Ακόμη και η αναγνώριση της γης απαιτεί ακόμη αναγνώριση της αρμόδιας δικαιοδοσίας.

Για να δώσω ένα άλλο σημείο, μια ράβδος χρυσού δεν μπορεί να κινηθεί. Ο ψηφιακός κριτής μπορεί να καθοδηγεί την κίνησή του, αλλά δεν μπορεί να το αναγκάσει χωρίς ανθρώπους να φιλοξενήσουν. Εξ ου και ένα ψηφιακό καθολικό μπορεί να απομακρυνθεί από την πραγματικότητα.

Έτσι, ένας σχεδιαστής πρωτοκόλλου πρέπει να αποφασίσει πόση ανθρώπινη πραγματικότητα πρέπει να επιτρέπεται στο κρυπτονόμισμα του. Όσο μεγαλύτερη ευελιξία, τόσο λιγότερη πιστότητα στο απόλυτο πρέπει να περιμένει κανείς. Όσο περισσότερη προστασία των καταναλωτών, τόσο περισσότεροι μηχανισμοί πρέπει να υπάρχουν για την παροχή επιστροφών, επιστροφών χρημάτων και επεξεργασίας του ιστορικού.

Αυτή η ενότητα και η επόμενη στον κανονισμό καλύπτει την πραγματιστική προσέγγιση του Cardano στο θέμα. Όσον αφορά τη διαλειτουργικότητα, υπάρχουν δύο ευρείες ομάδες για συζήτηση. Πρώτον, διαλειτουργικότητα με παλαιά χρηματοπιστωτικά συστήματα (ο κόσμος που δεν ανήκει σε κρυπτονομίσματα). Δεύτερον, διαλειτουργικότητα με άλλα κρυπτονομίσματα.

Κληρονομιά

Το Fintech δεν αποτελείται από ένα μόνο πρότυπο ή ακόμη και από μια κοινή γλώσσα. Υπάρχει τεράστια ποικιλομορφία στις προσεγγίσεις, στις οντότητες που είναι υπεύθυνες για διακανονισμό και εκκαθάριση, επιχειρηματικές διαδικασίες και άλλους τομείς που εμπλέκονται στη λογιστική, τη μετατροπή και την κίνηση της αξίας.

Είναι παράλογο να προτείνουμε ότι, απλώς και μόνο επειδή μια τεχνολογία είναι ανώτερη, το υπόλοιπο οικοσύστημα θα παραδεχθεί κάπως την ήττα και την αναβάθμιση. Για παράδειγμα, πολλά άτομα εξακολουθούν να χρησιμοποιούν τα Windows XP 16 χρόνια μετά την αρχική κυκλοφορία. Αυτή η θλιβερή κατάσταση είναι ισοδύναμη με κάποιον που χρησιμοποιεί το αρχικό Macintosh που κυκλοφόρησε το 1984 το 2000.

Εκτός από τη συμπεριφορά των καταναλωτών, οι επιχειρήσεις είναι γενικά ακόμη πιο αργές στον κύκλο αναβάθμισής τους. Πολλές τράπεζες εξακολουθούν να χρησιμοποιούν παρασκήνια γραμμένα στο Cobol. Μόλις η υποδομή είναι γνωστό ότι λειτουργεί και πληροί τις επιχειρηματικές απαιτήσεις, συνήθως υπάρχει ελάχιστο κίνητρο για αναβάθμιση ή βελτίωση λογισμικού και πρωτοκόλλων προς όφελος ενός καταναλωτή εκτός από θέματα συμμόρφωσης ή ασφάλειας.

Για το Cardano, πρέπει πρώτα να καθορίσουμε τι θα συνεπαγόταν μια γέφυρα παλαιού τύπου; Ποια συστήματα, πρότυπα, οντότητες και πρωτόκολλα πρέπει να στοχεύσουμε για να διασφαλίσουμε ότι υπάρχει εύλογη βεβαιότητα διαλειτουργικότητας; Μπορούν αυτές οι γέφυρες να ενοποιηθούν ή να αποκεντρωθούν; Ή όπως οι ανταλλαγές θα γίνουν κεντρικά σημεία αποτυχίας για χάκερ, κακόβουλους ιδιοκτήτες ή υπερβολικά ενθουσιώδεις ρυθμιστές;

Υπάρχουν τρεις ανησυχίες που πρέπει να αντιμετωπιστούν. Πρώτον, η αναπαράσταση των πληροφοριών και η πίστη στην ακρίβειά τους. Δεύτερον, αναπαράσταση της αξίας και της σχετικής ιδιοκτησίας. Τρίτον,

η εκπροσώπηση των οντοτήτων και, ενός συγκεκριμένου χρήστη παράλληλα με το συνολικό επίπεδο εμπιστοσύνης σε αυτές τις οντότητες.

Για να είναι χρήσιμες, οι πληροφορίες και η αξία πρέπει να ρέουν ελεύθερα μεταξύ του παλαιού οικονομικού κόσμου και του Cardano. Στη συνέχεια, τα αποτελέσματα πρέπει να καθοριστούν και να καταγραφούν για να οικοδομήσουμε τη φήμη και τους λόγους προσφυγής. Ωστόσο, τέτοια πράγματα έχουν ως επί το πλείστον τη φύση τους στους εμπλεκόμενους φορείς. Η κωδικοποίησή τους σε ένα blockchain θα τους έκανε καθολικούς και μόνιμους.

Επιπλέον, η αξία δεν μπορεί πάντα να ρέει ελεύθερα στον κόσμο της κληρονομιάς. Εμπάργο, κυρώσεις, έλεγχοι κεφαλαίου και δικαστική δράση θα μπορούσαν να παγώσουν περιουσιακά στοιχεία. Για να είναι διαλειτουργικό, δεν μπορεί κανείς να δημιουργήσει μια πάντα ανοιχτή βαλβίδα διαφυγής για διαρροή αξίας.

Τέλος, η επωνυμία και η φήμη των οντοτήτων είναι ένας από τους ακρογωνιαίους λίθους των εμπορικών σχέσεων. Δισεκατομμύρια δολάρια δαπανούνται ετησίως σε καμπάνιες μάρκετινγκ για τη δημιουργία, συντήρηση και επισκευή εμπορικών σημάτων. Εάν γίνονται δυσφημιστικοί, ψευδείς ή παραπλανητικοί ισχυρισμοί για ένα άτομο ή οντότητα, τότε έχουν το δικαίωμα να αναζητήσουν νομική προσφυγή. Ωστόσο, οι blockchain προσπαθούν να διατηρήσουν μόνιμα την ιστορία.

Όπως και η επιλογή της γλώσσας προγραμματισμού μας, δεν υπάρχει ιδανική λύση για το Cardano να επιλύσει αυτές τις ανησυχίες με σχεδόν παντού σωστό τρόπο. Αντίθετα, πρέπει να υποχωρήσουμε ξανά στην υποστηριζόμενη γνώμη.

Όσον αφορά τη ροή πληροφοριών, αυτή η ροή είναι γνωστή ως αξιόπιστη ροή δεδομένων. Έχει πηγή και περιεχόμενο. Οι πηγές έχουν κάποια έννοια αξιοπιστίας και κίνητρο να εξαπατήσουν ή να διατηρήσουν την ειλικρίνεια. Το περιεχόμενο μπορεί να κωδικοποιηθεί αυθαίρετα.

Δεδομένου ότι σκοπεύουμε να υποστηρίξουμε αξιόπιστο υλικό στη στοίβα πρωτοκόλλων μας, επιλέξαμε να διερευνήσουμε την προσθήκη υποστήριξης για το πρωτόκολλο Town Crier του καθηγητή Ari Juel et al. Υποθέτοντας την ύπαρξη ενός αξιόπιστου συνόλου πηγών δεδομένων, το Town Crier επιτρέπει την ασφαλή απόσυρση περιεχομένου Ιστού για χρήση σε έξυπνες συμβάσεις και άλλες εφαρμογές.

Μια λίστα με πηγές bootstrap θα παρέχεται από τους Emurgo, IOHK και το Cardano Foundation. Αργότερα αυτή η λίστα θα αντικατασταθεί από μια λίστα επιμέλειας κοινότητας χρησιμοποιώντας μηχανικούς που προέρχονται από το σύστημα ταμείου του Cardano. Ελπίζουμε ότι ένα σύστημα φήμης μπορεί να υλοποιηθεί γύρω από καλές ροές δεδομένων, δημιουργώντας έτσι έναν θετικό βρόχο ανατροφοδότησης για τη σταδιακή βελτίωση της αξιοπιστίας και της πιστότητας.

Η αναπαράσταση της αξίας είναι ένα πιο περίπλοκο θέμα. Σε αντίθεση με τις πληροφορίες - όπου όταν διαπιστωθεί η αλήθεια, η επικαιρότητα και η πληρότητα, τα πρωτόκολλα μπορούν να συμπεριφέρονται με αξιόπιστο και ντετερμινιστικό τρόπο - η τιμή είναι πιο ευαίσθητη.

Μόλις αναγνωριστεί, η τιμή θα πρέπει να συμπεριφέρεται σαν ένα μοναδικό αντικείμενο. Οι πληροφορίες μπορούν να αντιγραφούν και να μεταδοθούν, αλλά ένα διακριτικό που αντιπροσωπεύει

την κυριότητα κάτι (ας πούμε έναν τίτλο οχήματος) δεν μπορεί να κλωνοποιηθεί και να ανταλλαχθεί σε δύο διαφορετικά καθολικά. Αυτή η πράξη θα καταστρέψει αποτελεσματικά την ακεραιότητα του συστήματος.

Η πρόκληση στην κληρονομική διαλειτουργικότητα όταν ασχολείστε με την ονομαστική αξία είναι ότι οι παραδοχές εμπιστοσύνης, η αξιοπιστία και η δυνατότητα ελέγχου αλλάζουν καθώς οι μάρκες ρέουν μεταξύ των καθολικών. Για παράδειγμα, εάν ο Μπομπ κατέχει κάποιο Bitcoin και έπειτα τα καταθέσει σε ανταλλακτήριο, τότε ο Μπομπ έχει τώρα την αναπαράσταση της ανταλλαγής για το Bitcoin του στο καθολικό τους. Στην περίπτωση του MtGOX, το καθολικό τους δεν ανταποκρίθηκε στην πραγματικότητα, με αποτέλεσμα οι χρήστες να χάσουν τα πάντα.

Το πρόβλημα περιπλέκεται περαιτέρω από την ανάγκη για συστήματα παλαιού τύπου να αναγνωρίζουν μάρκες που ζουν σε κρυπτονομίσματα. Όπως αναφέρθηκε προηγουμένως, οι επιχειρήσεις είναι ιστορικά ανθεκτικές στην αναβάθμιση του λογισμικού τους και την υποστήριξη νέων πρωτοκόλλων. Αυτή η κατάσταση καθιστά δύσκολο να δούμε μια σαφή λύση.

Για το Cardano, η καλύτερη ελπίδα μας είναι να παρέχουμε μια επιλογή στους χρήστες να συνδέσουν μια πλούσια παροχή μεταδεδομένων στις συναλλαγές τους και στη συνέχεια να περιμένουν να εμφανιστούν πρότυπα βιομηχανίας. Έχει σημειωθεί κάποια πρόοδος στην ομάδα εργασίας του Interledger, προσπάθειες όπως το R3Cev και διεθνείς εντολές για την αναβάθμιση παλαιών οικονομικών πρωτοκόλλων.

Ωστόσο, η μεγαλύτερη πρόκληση παραμένει της ποσοτικοποίησης και της αξίας που αποστέλλεται από ένα κληρονομικό σύστημα σε ένα κρυπτονόμισμα. Για παράδειγμα, εάν ο Μπομπ είναι κάτοχος τράπεζας και εκδίδει ένα token που υποστηρίζεται από το δολάριο, τότε μπορεί πάντα να χτίσει μια γέφυρα για να στείλει τα tokens του σε ένα βιβλίο όπως το Cardano ως στοιχείο που έχει εκδοθεί από τον χρήστη.

Ενώ το Cardano θα παρακολουθούσε με ακρίβεια την ιδιοκτησία και θα παρέχει όλες τις δυνατότητες που έχουμε αγαπήσει, όπως η χρονική σήμανση και η δυνατότητα ελέγχου, κανένα κρυπτονόμισμα δεν μπορεί να κάνει τον Bob έναν έντιμο τραπεζίτη. Έχει πάντα την επιλογή να τρέξει μια κλασματική τράπεζα αποθεματικών χωρίς να υποστηρίζει όλα τα tokens του δολαρίου του με πραγματικά δολάρια. Αυτή η απάτη δεν μπορεί να εντοπιστεί από ένα κρυπτονόμισμα, εκτός εάν το ίδιο το δολάριο ήταν ένα token που υπολογίζεται από ένα ψηφιακό καθολικό.

Τέλος, η εκπροσώπηση οντοτήτων στο διαδίκτυο είναι ένα κλασικό πρόβλημα δικτύου που χρονολογείται από τις πρώτες μέρες του Διαδικτύου. Τα πανεπιστήμια, οι επιχειρήσεις, τα κυβερνητικά τμήματα και τυχόν αυθαίρετοι χρήστες πρέπει να προσδιορίσουν την ταυτότητά τους κάποια στιγμή.

Για το σκοπό αυτό, έχουν υλοποιηθεί ρεαλιστικές αλλά συγκεντρωτικές λύσεις, όπως η υποδομή δημόσιου κλειδιού και το σύστημα DNS του ICANN. Δεδομένου ότι απολαμβάνουμε τον σύγχρονο ιστό, αυτές οι λύσεις είναι τόσο επεκτάσιμες όσο και πρακτικές. Αλλά δεν απαντούν σε ένα πιο εμπορικά προσανατολισμένο ζήτημα αξιοπιστίας, αξιοπιστίας και άλλων μετα-χαρακτηριστικών που είναι απαραίτητα για να προσδιοριστεί εάν κάποιος θέλει να συνεργαστεί με την οντότητα.

Οι κεντρικοί υπολογιστές πολλαπλών όψεων όπως το eBay έχουν δημιουργήσει ένα επιχειρηματικό μοντέλο για την παροχή ορισμένων από αυτά τα μεταδεδομένα παράλληλα με ένα πλαίσιο για την ολοκλήρωση των συναλλαγών. Οι κρίσεις σχετικά με την ποιότητα του περιεχομένου, των εκδηλώσεων και των επιχειρήσεων επηρεάζονται συχνά βαθιά αποκλειστικά από διαδικτυακές αξιολογήσεις από αξιόπιστες πηγές.

Το μέρος αυτού του σημείου που σχετίζεται με το Cardano είναι ένα ζήτημα συγκεντρωτισμού της φήμης. Ένας από τους στόχους μας για το Cardano είναι να παρέχουμε μια οικονομική στοίβα για τον αναπτυσσόμενο κόσμο. Ένα κλειδί σε αυτήν την προσπάθεια είναι η ικανότητα να δημιουργηθεί εμπιστοσύνη με φορείς που δεν έχει γνωρίσει ποτέ.

Εάν μια μεμονωμένη οντότητα ή μια κοινοπραξία οντοτήτων ελέγχει ποιος χαρακτηρίζεται καλός ή κακός, όχι οργανική διαδικασία που προέρχεται από πραγματικές αλληλεπιδράσεις στην κοινότητα στο σύνολό της, τότε αυτές οι οντότητες θα μπορούσαν αυθαίρετα να αποκλείσουν οποιονδήποτε για τυχόν αντιληπτή αμαρτία. Αυτή η δύναμη έρχεται σε αντίθεση με τις αξίες μας ως έργο και νικά το ευρύτερο σημείο της χρήσης κρυπτογράφησης.

Ευτυχώς, οι ίδιοι μηχανισμοί που χρησιμοποιήθηκαν στην ψηφοφορία για τα ψηφοδέλτια θησαυρού, προσθέτοντας πηγές σε μια λίστα αξιόπιστων ροών δεδομένων και διαμορφώνοντας ένα πρωτόκολλο μπορούν να επαναχρησιμοποιηθούν για να δημιουργηθεί ένας χώρος φήμης. Είναι ένας ανοιχτός χώρος έρευνας και ελπίζουμε να παρέχουμε ένα πρωτόκολλο επικάλυψης για έναν αποκεντρωμένο ιστό αξιοπιστίας φήμης το 2018-2019 μετά την επίλυση περισσότερων θεμελιωδών στοιχείων.

Κρυπτονομίσματα και διαλειτουργικότητα

Μεταβαίνοντας από τον παλαιό κόσμο σε κατανεμημένα ψηφιακά καθολικά, η διαλειτουργικότητα γίνεται πολύ πιο απλή. Κάθε καθολικό διαθέτει ένα πρωτόκολλο δικτύου, πρότυπα επικοινωνίας και παραδοχές ασφάλειας σχετικά με τον αντίστοιχο αλγόριθμο συναίνεσης. Αυτά με τη σειρά τους μπορούν να ποσοτικοποιηθούν εύκολα.

Η κυκλοφορία των πληροφοριών πραγματοποιείται συνδέοντας στο ξένο δίκτυο και μεταφράζοντας τα μηνύματά του. Η μετακίνηση της αξίας μπορεί να γίνει μέσω ενός συστήματος ρελέ, ανταλλαγής ατομικών διαγώνιων αλυσίδων ή μέσω ενός έξυπνου σχήματος πλευρικών αλυσίδων. Δεδομένου ότι δεν υπάρχει κεντρικός χειριστής, μια εκπροσώπηση οντοτήτων περιορίζει περισσότερο σε ένα μέσο εμπιστοσύνης σε προγραμματιστές, ανθρακωρύχους ή σε κάποιον άλλο μεσίτη ισχύος.

Για το Cardano, ενσωματώνουμε ένα νέο πρωτόκολλο sidechain που αναπτύχθηκε από τους Kiayias, Miller και Zindros. Παρέχει έναν μη διαδραστικό τρόπο ασφαλούς μετακίνησης της αξίας μεταξύ δύο αλυσίδων που υποστηρίζουν το πρωτόκολλο. Αυτός ο μηχανισμός θα είναι ο πρωτεύων τρόπος ροής μεταξύ CSL και ενός επιπέδου CCL.

Για άλλα κρυπτονομίσματα, οι ενοποιημένες γέφυρες θα πρέπει να σχηματίζονται καθώς το Cardano αυξάνεται σε αξία και βάση χρηστών. Για να επιταχυνθεί αυτή η ανάπτυξη, το Cardano SL υποστηρίζει

μια περιορισμένη έκδοση του Plutus για σενάρια διαλειτουργικότητας. Νέες συναλλαγές θα προστεθούν στο Shelley και σε μεταγενέστερες εκδόσεις του CSL ειδικά για την αντιμετώπιση αυτών των αναγκών.

Ο λαβύρινθος του Daedalus

Τα σημεία διαλειτουργικότητας προέρχονται από μια παγκόσμια προοπτική. Τα εξειδικευμένα πρωτόκολλα, οι νέοι τύποι συναλλαγών, τα συστήματα αξιολόγησης της αξιοπιστίας και η ροή πληροφοριών δεν μπορούν να καλυφθούν σε μία μόνο πύλη ή έναν χρήστη. Αντίθετα, πρέπει να είναι άμεσα διαθέσιμα σε οποιονδήποτε χωρίς λογοκρισία ή διόδια.

Ωστόσο, τι συμβαίνει όταν το Cardano δεν υποστηρίζει πρωτόκολλο, συναλλαγή ή εφαρμογή που δεν μπορεί να ζήσει ένας χρήστης; Πρέπει απλώς να μην είμαστε εκτός πεδίου; Ο ιστός αντιμετώπισε παρόμοια ανησυχία κατά τη δεκαετία του 1990.

Κατά ειρωνικό τρόπο, ο ιστός παρέχει δύο διαφορετικές λύσεις που μπορούν να αναπαραχθούν με κρυπτονομίσματα. Η εισαγωγή του JavaScript παρείχε δυνατότητα προγραμματισμού σε οποιονδήποτε ιστότοπο για την προσθήκη αυθαίρετων λειτουργιών. Η εισαγωγή προσθηκών και επεκτάσεων προγράμματος περιήγησης πρόσθεσε προσαρμοσμένες δυνατότητες για χρήστες που επιθυμούν να τις εγκαταστήσουν. Και οι δύο προσεγγίσεις μας έδωσαν τον σύγχρονο ιστό παράλληλα με όλες τις φρίκης ασφαλείας.

Το Ethereum υιοθέτησε την προηγούμενη προσέγγιση επιτρέποντας στους χρήστες να ενσωματώσουν υπο-πρωτόκολλα στο blockchain Ethereum ως έξυπνα συμβόλαια. Το Cardano υποστηρίζει αυτήν τη δυνατότητα μέσω του παραδείγματος CCL. Τι γίνεται όμως με τις προσαρμοσμένες επεκτάσεις;

Ένα διευκρινιστικό παράδειγμα θα ήταν ένας έμπορος κρυπτονομισμάτων. Φανταστείτε μια αποκεντρωμένη αγορά, που ονομάζεται DM, που υποστηρίζει ένα σύνολο διαφορετικών κρυπτονομισμάτων. Ένας έμπορος θέλει να αυτοματοποιήσει τις στρατηγικές του ενεργώντας στο DM.

Σε ένα κατακερματισμένο οικοσύστημα, ο έμπορος θα πρέπει να εγκαταστήσει δεκάδες πελάτες για κάθε κρυπτονόμισμα και στη συνέχεια να γράψει προσαρμοσμένο λογισμικό για να μιλήσει σε κάθε πελάτη προκειμένου να συντονίσει τις αυτόματες συναλλαγές. Εάν ένας πελάτης ενημερώσει, τότε θα μπορούσε να σπάσει το λογισμικό κατά παραγγελία. Επιπλέον, τι γίνεται αν ο έμπορος θέλει να πουλήσει το λογισμικό;

Εμπνευσμένο από το μοντέλο επεκτάσεων ιστού, εάν η διεπαφή σε διάφορα κρυπτονομίσματα μπορεί να τραβηχτεί σε μια στοίβα ιστού, τότε η εργασία του εμπόρου γίνεται δραματικά ευκολότερη. Μπορεί να δημιουργηθεί μια καθολική διεπαφή. Η εγκατάσταση είναι ένα κλικ. Η διανομή λογισμικού μπορεί να μοντελοποιηθεί μετά το Chrome web store.

Για το Cardano, αποφασίσαμε να πειραματιστούμε με αυτό το παράδειγμα αναπτύσσοντας το μπροστινό άκρο του πορτοφολιού αναφοράς μας στο Electron. Πρόκειται για ένα έργο ανοιχτού κώδικα που συντηρείται από το Github και συνδυάζει ταυτόχρονα το Node και το Chrome. Η κατασκευή του Cardano του Electron ονομάζεται Daedalus.

Η πρώτη γενιά του Daedalus θα λειτουργήσει ως πορτοφόλι HD με υποστήριξη για πολλά από τα αναμενόμενα χαρακτηριστικά λογιστικής και ασφάλειας που είναι πρότυπα του κλάδου, όπως κωδικοί πρόσβασης δαπανών και BIP39. Στις επόμενες γενιές, το Daedalus θα εξελιχθεί σε ένα πλαίσιο εφαρμογής με ένα κατάστημα, API καθολικής ολοκλήρωσης και ένα SDK.

Οι βασικές καινοτομίες είναι η ευκολία ανάπτυξης, επιτρέποντας στους προγραμματιστές να χρησιμοποιούν JavaScript, HTML5 και CSS3 για τη δημιουργία των εφαρμογών τους και μια ενοποιημένη γέφυρα για επικοινωνία μεταξύ εφαρμογών. Η περίπλοκη συμπεριφορά όπως η κρυπτογραφία, η διαχείριση ενός κατανεμημένου δικτύου και οι μηχανική βάσεων δεδομένων μπορούν να αφαιρεθούν, επιτρέποντας έτσι στον προγραμματιστή να επικεντρωθεί αποκλειστικά στην εμπειρία χρήστη και στη βασική λογική της εφαρμογής τους.

Καθώς το Daedalus προορίζεται να είναι ένα παγκόσμιο πλαίσιο, ο χάρτης πορείας και η εξέλιξή του είναι κάπως ανεξάρτητοι από το Cardano. Κατά τη διάρκεια του 2017 συνδέονται στενά, αλλά αργότερα το Cardano θα είναι απλώς μια άλλη εφαρμογή για έναν χρήστη του Daedalus. Σκοπεύουμε επίσης να διερευνήσουμε εξαιρετικά μοναδικά χαρακτηριστικά, όπως μια καθολική υπηρεσία διαχείρισης κλειδιών που λειτουργεί αποκλειστικά στην Intel SGX.

Τελικά, ως σχεδιαστές πρωτοκόλλων, δεν μπορούμε να υποστηρίξουμε όλες τις ανάγκες. Η ελπίδα μας είναι ότι η ευελιξία που θα προσφέρει η Daedalus σε συνδυασμό με έξυπνα συμβόλαια που λειτουργούν στο CCL θα ικανοποιήσει αυτά που έχουν μείνει από τις αποφάσεις σχεδιασμού μας. Ελπίζουμε επίσης ότι θα προκύψουν καλύτερα πρότυπα για να ενθαρρύνουν όλα τα κρυπτονομίσματα να απολαμβάνουν καλύτερη διαλειτουργικότητα και ασφάλεια.

Κανονιστικό πλαίσιο

Η λανθασμένη διχοτόμηση

Όσο ασταθής συχνά μπορεί να είναι ο κανονισμός, μπορεί κανείς να εκφράσει μεταφορικά έναν κομψό αφηγηματικό βρόχο των διεφθαρμένων και των εισαγγελέων τους που αναζητούν δικαιοσύνη. Οι κανονισμοί είναι η εργαλειοθήκη του νομικού προσώπου. Όμως, όπως όλα τα εργαλεία, μπορεί να είναι ακατέργαστα, παλιά ή απλά να χρησιμοποιούνται κατά λάθος.

Τα κρυπτονομίσματα δεν έχουν αλλάξει την ανθρώπινη κατάσταση ή τον αφηγηματικό βρόχο. Θα υπάρχουν πάντα απάτες, κακοί χειριστές και φοβερά αποτελέσματα παρά τις καλύτερες προθέσεις. Ενώ τα κρυπτονομίσματα μπορούν να αφαιρέσουν την ανθρώπινη κρίση, δεν μπορούν να αφαιρέσουν την ανθρώπινη συμπεριφορά.

Ένας σχεδιαστής κρυπτονομισμάτων πρέπει να λάβει θέση σχετικά με το τι κιτ εργαλείων θα προσφέρει στον ρυθμιστή για τη διόρθωση κακών γεγονότων. Η μοναδική πρόκληση που αντιμετωπίζουν τα κρυπτονομίσματα είναι ότι είναι προϊόν ρυθμιστικής και νομισματικής αποτυχίας.

Πολιτιστικά, πολλοί σε κρυπτονομίσματα θεωρούν ότι η κυβερνητική δράση είναι διεφθαρμένη, ανίκανη ή αναποτελεσματική. Επομένως, έχουν ελάχιστο σεβασμό, υπομονή ή επιθυμία να εγκρίνουν μια ειδική πόρτα για μια ρυθμιστική αρχή ή έναν νομικό για να διορθώσει τα λάθη. Αυτή η πράξη θα ήταν ένα ανάθεμα για ολόκληρο τον σκοπό των κρυπτονομισμάτων.

Από την άλλη πλευρά, μετρώντας τις αποτυχίες ανταλλαγής και τα ιστορικά γεγονότα, περισσότερο από το 10 τοις εκατό του Bitcoin έχει χαθεί ή κλαπεί από το πρωτόκολλο που ξεκίνησε στις 3 Ιανουαρίου 2009. Από τις 30 Ιουνίου 2017, η αξία που χάθηκε ή κλαπεί φτάνει λίγο περισσότερο 4 δισεκατομμύρια δολάρια. Και αυτός ο αριθμός δεν αντιπροσωπεύει το Bitcoin και άλλα διακριτικά που χάθηκαν από απάτες και κακή διαμόρφωση ICO.

Τότε υπάρχει το ζήτημα της ιδιωτικής ζωής. Σε μακροοικονομική κλίμακα, η αξία ρέει μέσω εξειδικευμένων καναλιών που ρυθμίζονται, πλούσια σε μεταδεδομένα και παρακολουθούνται ενεργά από την επιβολή του νόμου, από κυβερνήσεις και διεθνείς ρυθμιστικές αρχές. Είναι ένα καλά κατανοητό παιχνίδι με διαρροή που συμβαίνει μόνο στην πλευρά των ταμειακών υποθέσεων, το οποίο σταδιακά μειώνεται καθώς ο κόσμος κινείται στο ψηφιακό χρήμα.

Το παράδειγμα εάν δεν υπήρχαν κρυπτονομίσματα φαίνεται να είναι ένας κόσμος που αντιμετωπίζει όλο και περισσότερο το οικονομικό απόρρητο όπως το περιεχόμενο των κοινωνικών μέσων. Δεν υπάρχει κανένα και δεν μπορεί κανείς να εξαιρεθεί. Ως εκ τούτου έχουμε ένα δίλημμα που αποδίδει μια φαινομενική διχοτόμηση.

Ένας σχεδιαστής κρυπτονομισμάτων μπορεί να παραδώσει τις αρχές και να παραδοθεί σε ό,τι απαιτεί η τοπική δικαιοδοσία του από τον κώδικά τους, υπονομεύοντας έτσι το απόρρητο και την ακεραιότητα των χρηστών τους. Ή μπορεί να υιοθετήσει μια πιο βασισμένη, αλλά αναρχική, φιλοσοφία που χωρίζεται από τις τρέχουσες βέλτιστες πρακτικές και νόμους.

Για το Cardano, πιστεύουμε ότι αυτή η αφήγηση είναι μια λανθασμένη διχοτόμηση που οφείλεται στην έλλειψη φαντασίας. Η πραγματικότητα είναι ότι οι περισσότεροι χρήστες δεν ενδιαφέρονται για τους κανόνες που ισχύουν για τις αγορές. Ανησυχούν συνήθως για ξαφνικές αλλαγές στους κανόνες που ωφελούν έναν ή περισσότερους συμμετέχοντες. Ανησυχούν για έλλειψη διαφάνειας σχετικά με το ποιος αποκτά ειδικά προνόμια.

Πρέπει να κάνουμε διάκριση μεταξύ των ατομικών και των δικαιωμάτων της αγοράς. Δεδομένου ότι τα κρυπτονομίσματα έχουν παγκόσμια εμβέλεια, τα δικαιώματα πρέπει να είναι όσο το δυνατόν πιο προσανατολισμένα στον χρήστη.

Το απόρρητο θα πρέπει να είναι λογικό και υπό τον έλεγχο του χρήστη και όχι ως φύλακας. Η ροή της αξίας πρέπει να είναι απεριόριστη. Η αξία δεν πρέπει να υπόκειται σε ξαφνική απώλεια χωρίς συγκατάθεση.

Από την πλευρά της αγοράς, η αγορά πρέπει να είναι διαφανής σχετικά με τη χρήση δεδομένων, πώς θα διαχειρίζονται τα κεφάλαια και όλοι πρέπει να παίζουν με το ίδιο σύνολο κανόνων. Επιπλέον, όταν ο χρήστης συναινέσει, τότε δεν μπορεί ξαφνικά να αλλάξει γνώμη λόγω ταλαιπωρίας. Οι αντισυμβαλλόμενοι χρειάζονται επίσης βεβαιότητα.

Αλλά πώς ακριβώς κινείται κάποιος από το αφηρημένο σε ένα πραγματικό σύστημα; Πώς πρέπει να μοιάζει κάτι πρακτικό και νομικό; Διαχωρίσαμε τη λύση μας σε τρεις κατηγορίες: μεταδεδομένα, έλεγχος ταυτότητας και συμμόρφωση, καθώς και DAO στην αγορά.

Μεταδεδομένα

Η πράξη για κάτι μπορεί συχνά να είναι λιγότερο ενδιαφέρουσα από τα μεταδεδομένα που την περιβάλλουν. Για παράδειγμα, η οδήγηση από το Ντένβερ στο Boulder είναι πράξη. Η οδήγηση από το Ντένβερ στο Boulder με Ferrari 488 με μέσο όρο 120 MPH είναι μεταδεδομένα. Σίγουρα αυτό προσφέρει μια διαφορετική εμπειρία από ό,τι σε ένα Toyota Prius κατά μέσο όρο 30 MPH.

Οι χρηματοοικονομικές συναλλαγές δεν διαφέρουν. Το πλαίσιο που τους περιβάλλει είναι εξαιρετικά σημαντικό για τους οικονομολόγους, τις φορολογικές αρχές, τις αρχές επιβολής του νόμου, τις επιχειρήσεις και άλλες οντότητες. Δυστυχώς, στο τρέχον σύστημά μας βασισμένο σε fiat, οι περισσότεροι καταναλωτές δεν βλέπουν ποτέ πόσο πλούσια σε μεταδεδομένα είναι οι συναλλαγές τους ή με ποιον μοιράζονται.

Για το Cardano, αναγνωρίζουμε ότι οι χρήστες θα μπορούσαν να χρειάζονται ή να είναι νομικά υποχρεωμένοι να μοιράζονται μεταδεδομένα συναλλαγών με ορισμένους φορείς όπως οι φορολογικές αρχές. Πιστεύουμε, ωστόσο, ότι αυτή η κοινή χρήση πρέπει να γίνεται κατόπιν συγκατάθεσης του χρήστη.

Πιστεύουμε επίσης ότι τα συστήματα blockchain έχουν τεράστια ισχύ για την εξάλειψη της απάτης, της σπατάλης και της κατάχρησης παρέχοντας δυνατότητα ελέγχου, χρονική σήμανση και αμετάβλητο. Έτσι, ορισμένα μεταδεδομένα θα πρέπει να δημοσιεύονται στο blockchain Cardano.

Το δύσκολο μέρος είναι να βρούμε μια σωστή ισορροπία που δεν καταδικάζει το blockchain μας σε σημαντικό “φούσκωμα”. Δεδομένης αυτής της ανησυχίας, επιλέξαμε μια ρεαλιστική προσέγγιση.

Πρώτον, το Daedalus θα υποστηρίξει τους επόμενους 12 μήνες μια μεγάλη γκάμα χαρακτηριστικών για την επισήμανση συναλλαγών και οικονομικής δραστηριότητας. Αυτά τα μεταδεδομένα μπορούν να εξαχθούν και να κοινοποιηθούν κατ' απαίτηση με όποιον ο χρήστης κρίνει απαραίτητο. Επιπλέον, τα δεδομένα μπορούν να χρησιμοποιηθούν από εφαρμογές τρίτων για συγκεκριμένους τομείς (για παράδειγμα, φορολογική λογιστική).

Δεύτερον, διερευνούμε την προσθήκη υποστήριξης για ειδικές διευθύνσεις που μπορούν να περιλαμβάνουν κατακερματισμούς και κρυπτογραφημένα πεδία. Αυτή η δομή θα επιτρέπει σε έναν χρήστη να δημοσιεύει μεταδεδομένα στο blockchain μας χωρίς να τα αποκαλύπτει δημόσια. Αλλά αν θέλει να μοιραστεί τα δεδομένα, θα φέρει όλη την ελεγκσιμότητα, το αμετάβλητο και τη χρονική σήμανση που απολαμβάνει μια συναλλαγή.

Έχουμε ήδη αναπτύξει μια δομή διευθύνσεων που περιέχει ένα πεδίο χαρακτηριστικών. Αυτή τη στιγμή χρησιμοποιείται για την αποθήκευση ενός κρυπτογραφημένου αντιγράφου της δομής δέντρων

πορτοφολιών HD για γρήγορη ανάκτηση πορτοφολιών (βλ. Τεκμηρίωση του Πορτοφολιού HD). Οι μεταγενέστερες εκδόσεις θα γενικεύσουν αυτήν την κατασκευή

Αυθεντικότητα και συμμόρφωση

Συνδεόμενα στενά με τις συναλλαγές είναι τα θέματα του δικαιώματος πραγματοποίησης συναλλαγών και της ιδιοκτησίας κεφαλαίων. Για παράδειγμα, ενώ μπορεί να υπάρχουν αρκετά χρήματα για να αγοράσετε κάτι (για παράδειγμα αλκοόλ), ενδέχεται να υπάρχουν περιορισμοί στην αγορά του (απαιτήσεις ηλικίας).

Η ιδιοκτησία και η προέλευση των κεφαλαίων είναι συνήθως παροχή γνώσης των κανονισμών πελατών σας. Όταν μια επιχείρηση παροχής χρημάτων όπως μια τράπεζα ή ένα χρηματιστήριο ανοίγει έναν λογαριασμό για έναν νέο πελάτη, συνήθως απαιτείται η συλλογή βασικών στοιχείων για τον πελάτη και από πού απέκτησε τα χρήματά του.

Η τεχνολογική πρόκληση είναι ότι κατά τη διαδικασία υποβολής αυτών των νομικά απαιτούμενων πληροφοριών, ο χρήστης που τις στέλνει δεν έχει καμία εγγύηση πώς θα χρησιμοποιηθούν, θα αποθηκευτούν και εάν θα καταστραφούν ποτέ. Οι πληροφορίες συμμόρφωσης είναι εμπορικά πολύτιμες. Θα μπορούσε να κλαπεί για κλοπή ταυτότητας ή να μεταπωληθεί όπου το επιτρέπουν οι κανονισμοί.

Για το Cardano, θέλουμε να καινοτομούμε όσο το δυνατόν περισσότερο. Από την πλευρά του λογισμικού των πρωτοκόλλων, δεν υπάρχει καμία εγγύηση ότι ο παραλήπτης πληροφοριών συμμόρφωσης θα συμπεριφέρεται εντός ενός πεδίου συμπεριφοράς. Ωστόσο, από την πλευρά του υλικού των πρωτοκόλλων, χρησιμοποιώντας αξιόπιστο υλικό, μπορεί κανείς να αξιοποιήσει την Intel SGX και άλλα HSM για την επιβολή συγκεκριμένων πολιτικών.

Συνεπώς, διερευνούμε τη χρήση σφραγισμένων γυαλιών απόδειξης (“Sealed glass proofs”) παράλληλα με μια πολιτική κοινής χρήσης που επιτρέπει την ασφαλή μετάδοση πληροφοριών συμμόρφωσης σε έναν επαληθευτή ο οποίος με τη σειρά του αναγκάζεται να συμμορφωθεί με τις πολιτικές στις οποίες διαβιβάστηκε. Πιστεύουμε ότι θα μπορούσαν να προκύψουν και τα δύο ομοιόμορφα πρότυπα και επίσης ότι αυτή η μέθοδος θα μειώσει τον κίνδυνο για επαληθευτές, αποτρέποντας την απώλεια δεδομένων πελατών από χάκερ.

Ως συνέπεια αυτής της προσπάθειας, το πολυεπίπεδο μοντέλο που προτείνουμε για το Cardano που διαχωρίζει την τιμή από τον υπολογισμό μπορεί επίσης να επωφεληθεί από αυτήν την προσέγγιση. Εάν το επίπεδο υπολογισμού διευθύνεται από ρυθμιζόμενες οντότητες (π.χ. ανταλλαγές ή καζίνο), τότε θα πρέπει να διενεργούν ελέγχους συμμόρφωσης και ενδεχομένως να επιβάλλουν φορολογική πολιτική στους χρήστες.

Χρησιμοποιώντας SGP, ο χρήστης μπορεί να στείλει χρήματα μαζί με προσωπικά αναγνωρίσιμες πληροφορίες χωρίς να ανησυχεί ότι θα διαρρεύσει στο ευρύτερο Διαδίκτυο ή θα διατηρηθεί από τους

κόμβους συναίνεσης του επιπέδου υπολογισμού. Επιπλέον, το επίπεδο υπολογισμού θα αποκτήσει βεβαιότητα ότι όλοι οι χρήστες που πραγματοποιούν συναλλαγές είναι αυθεντικοί και νόμιμοι.

Αυτό το παράδειγμα επιτρέπει επίσης τη φορητότητα των πελατών μεταξύ ρυθμιζόμενων οντοτήτων. Οι ανταλλαγές θα μπορούσαν να μεταφέρουν υπόλοιπα και λογαριασμούς για πελάτες άμεσα μέσω αυτών των ασφαλών καναλιών και επίσης - όπου το επιτρέπουν οι πολιτικές - να κοινοποιούν δεδομένα σε ρυθμιστικές αρχές.

Αναμένουμε ότι η πρώτη δοκιμή beta αυτής της τεχνολογίας θα διεξαχθεί στα μέσα του 2018 με στόχο την ολοκλήρωση τoy Cardano στα τέλη του 2018 έως τις αρχές του 2019 εν αναμονή των ερευνητικών αποτελεσμάτων. Αυτό το χρονοδιάγραμμα προϋποθέτει επίσης τη δυνατότητα συνεργασίας με ARM και Intel προκειμένου να υπογραφεί κώδικας για να εκτελεστεί στο υλικό τους.

Marketplace DAOs

Οι δύο προηγούμενες ενότητες κάλυψαν τη δημιουργία και την κίνηση πληροφοριών, υποθέτοντας ότι υπάρχει κάποιο εξωτερικό σύστημα. Για να διασφαλιστεί η διαλειτουργικότητα παλαιού τύπου, αυτές οι λειτουργίες θα είναι πάντοτε απαραίτητες, αλλά δεν αφορούν κανονισμούς που βασίζονται σε blockchain.

Τα έξυπνα συμβόλαια επιτρέπουν ένα εντελώς νέο είδος εμπορικού συστήματος όπου οι σχέσεις είναι ντετερμινιστικές, αυτο-επιβεβλημένες και χωρίς αμφισημία. Μπορούν με τη σειρά τους να χρησιμοποιηθούν για τη δημιουργία κανόνων για αγορές, συμπεριλαμβανομένων αυθαίρετων σύνθετων δομών όπως διαιτησία, επιστροφές βάσει συμβάντων και αποκάλυψη γεγονότων με ειδικούς όρους.

Ονομάζουμε αυτές τις έξυπνες δομές που επιβάλλονται από συμβόλαια Marketplace DAOs. Δεν απαιτούν ειδική υποστήριξη πρωτοκόλλου ούτε μεταβλητότητα για να ενσωματωθούν στο καθολικό. Στην πραγματικότητα, μπορούν να κατασκευαστούν πλήρως χρησιμοποιώντας μια συλλογή αλληλοεξαρτώμενων έξυπνων συμβάσεων.

Η αρχιτεκτονική ιδέα είναι να σχεδιάσουμε μια συλλογή εμπορικών προτύπων εμπνευσμένων από το δίκαιο των συμβάσεων και τις βέλτιστες επιχειρηματικές πρακτικές. Αυτά τα πρότυπα μπορούν να ενταχθούν σε μια έξυπνη σύμβαση προγραμματιστή για την επιβολή συγκεκριμένων προτύπων στην αγορά.

Για παράδειγμα, ας πούμε ότι ένας προγραμματιστής θέλει να εκδώσει ένα διακριτικό ERC20 στο CCL για να πραγματοποιήσει ένα πλήθος πωλήσεων. Ένα Marketplace DAO θα μπορούσε να δημιουργηθεί ειδικά για crowdsales και οι όροι και οι προϋποθέσεις του παραμετροποιούνται ή ακόμη και εφαρμόζονται από εθελοντικά ή νομικά πρότυπα. Πράγματα όπως επιστροφές χρημάτων, ανακατανομή χρημάτων ή δέσμευση πληρωμών θα μπορούσαν να κληρονομηθούν στη σύμβαση ERC20 του προγραμματιστή.

Αυτή η προσπάθεια μας επιτρέπει να κάνουμε μια μακριά συζήτηση για το πώς πρέπει να ελέγχεται μια αγορά προκειμένου να διασφαλίζεται η προστασία των καταναλωτών. Δεύτερον, μπορούμε να

συζητήσουμε πώς να μοντελοποιούμε συναλλαγές με τρόπο ώστε να διασφαλίζεται αυτόματα η νομική προστασία και τα δικαιώματα εντός συγκεκριμένων δικαιοδοσιών, όπως το New Hampshire.

Σε συνεργασία με το Cardano Foundation, το IOHK και άλλες οντότητες, το έργο Cardano θα δημιουργήσει μια βιβλιοθήκη αναφοράς του Marketplace DAO για χρήση έξυπνων συμβολαίων. Η ελπίδα μας είναι ότι οι ασφαλιστικές και ρυθμιστικές αγορές μπορούν να σχηματιστούν γύρω από αυτούς τους DAO και ότι θα εξελιχθούν μόνοι με βάση τα αποτελέσματα

Βιωσιμότητα

Η εμβάπτιση στην περιοχή κρυπτονομισμάτων αποφέρει πολλές εννοιολογικές αντιφάσεις. Τα κρυπτονομίσματα έχουν σχεδιαστεί για να είναι δύσκολο να αλλάξουν, αλλά, όπως και όλες οι τεχνολογίες, πρέπει να αλλάξουν για να αντιμετωπίσουν τα ελαττώματα και τις εξελίξεις στο σχεδιασμό τους. Τα blockchains προορίζονται να αποτρέψουν τη συγκέντρωση (centralization) , αλλά απαιτούν ισχυρούς παράγοντες να καθοδηγήσουν αλλαγές ή να διατηρήσουν τον κώδικα.

Ίσως η πιο απογοητευτική εμπειρία έρχεται όταν υπάρχουν σαφείς ελλείψεις που οι περισσότεροι ενδιαφερόμενοι συμφωνούν ότι πρέπει να διορθωθούν, ωστόσο η συναίνεση δεν μπορεί να προκύψει στη διαδρομή που θα ακολουθηθεί.

Η συζήτηση για το μέγεθος μπλοκ του Bitcoin αποτελεί πλέον ενεργό ζήτημα για περισσότερα από δύο χρόνια. Καθημερινά, εκκρεμούν συναλλαγές συνολικού ύψους άνω του ενός δισεκατομμυρίου δολαρίων, επειδή το δίκτυο έχει μέγιστη χωρητικότητα.

Εάν η αλλαγή μιας απλής παραμέτρου - ακόμη και παρουσία προσωρινών λύσεων - δεν μπορεί να συντονιστεί, τότε πώς μπορούν οι επιχειρήσεις και οι κυβερνήσεις να αισθάνονται άνετα ώστε να επενδύσουν δισεκατομμύρια δολάρια στην κατασκευή υποδομών πάνω σε αυτά τα συστήματα; Για αυτό το θέμα, πώς μπορεί κάθε επιχείρηση να στοιχηματίσει στον στρατηγικό κίνδυνο ενσωμάτωσης πρωτοκόλλων χωρίς λογοδοσία που δεν μπορούν να κάνουν οι ορθολογικές αναβαθμίσεις σχεδιασμού;

Κοιτάζοντας πίσω στην ιστορία, η εξέλιξη του Διαδικτύου ακολούθησε ένα παρόμοιο μοτίβο με ακόμη και απλές αλλαγές όπως η μετάβαση από το IPv4 στο IPv6 να χρειάζονται δεκαετίες για να πραγματοποιηθούν. Ωστόσο, υπάρχει μια έντονη αντίθεση μεταξύ της τεχνολογίας blockchain και του Διαδικτύου στο ότι ακολουθούν ένα πολύ διαφορετικό στυλ φύλαξης.

Το Διαδίκτυο ήταν ένα στρατιωτικό έργο που αναπτύχθηκε από το DARPA σε ακαδημαϊκούς κύκλους με ισχυρή κυβερνητική υποστήριξη και ένα καλά καθορισμένο σύνολο αρχικών θεματοφυλάκων. Το Διαδίκτυο αναπτύχθηκε κάτω από μη εμπορικές συνθήκες χωρίς τους μηχανισμούς εταιρικής επιρροής να προσπαθούν να μονοπωλήσουν το δίκτυο. Στην πραγματικότητα, το ηλεκτρονικό εμπόριο παραβίαζε το NSF AUP έως ότου καταργήθηκε το 1992.

Όταν οι επιχειρήσεις είχαν την πολυτέλεια να εμπορευματοποιήσουν το Διαδίκτυο, υπήρχε ήδη ένα ισχυρό σύνολο προτύπων, αρχών και ευαγγελιστών. Αυτό δεν εμπόδισε εταιρείες όπως η AOL και η

Microsoft να προσπαθήσουν να χτίσουν wall gardens (ο τρόπος με τον οποίο γίνεται σωστή διαχείριση των δεδομένων) και να δημιουργήσουν ιδιόκτητη τεχνολογία όπως το ActiveX. Αυτό το ίδρυμα δεν εμπόδισε τους ανταγωνιστές της επόμενης γενιάς, όπως η Google να προωθήσουν τις δικές τους ατζέντες, δεδομένης της τεράστιας βάσης χρηστών και κεφαλαιοποιήσεών τους.

Με μιλιούνια παράγοντες / ανθρώπους που ψάχνουν να βρουν να νοικιάσουν από traders μέχρι miners, τα κρυπτονομίσματα είναι τα απόλυτα εμπορικά οικοσυστήματα. Λαμβάνοντας υπόψη αυτό το θεμέλιο, η εξέλιξη της κηδεμονίας των κρυπτονομισμάτων έχει οδηγήσει σε βελτιστοποίηση γύρω από το συμφέρον.

Για παράδειγμα, η εξόρυξη χωρίς επικύρωση αρχίζει να συμβαίνει συχνότερα καθώς βελτιώνει το περιθώριο κέρδους ενός miner, αλλά αυτό αγνοεί πλήρως ολόκληρο τον σκοπό και τη χρησιμότητα της εξόρυξης. Η κεντρική εξόρυξη έχει ήδη συμβεί με λίγους παράγοντες που ελέγχουν την πλειονότητα της ισχύος κατακερματισμού του Bitcoin.

Όπως το Διαδίκτυο, έτσι και τα κρυπτονομίσματα απαιτούν συναίνεση για αλλαγή. Αλλά όταν συμβαίνει ένας τόσο γρήγορος συγκεντρωτισμός της εξουσίας σε μια χούφτα μεσίτες, τι θα συμβεί όταν η αλλαγή δεν είναι κατάλληλη για αυτούς;

Σε αντίθεση με το Διαδίκτυο, το bootstrapping των περισσότερων κρυπτονομισμάτων δεν γίνεται με αλτρουιστικά μη εμπορικά ή ακαδημαϊκά μέσα. Από την αρχή, κάποια ομάδα επιδιώκει να δημιουργήσει κέρδη και υπάρχουν εξουσιοδοτημένοι μεσίτες για να βοηθήσουν στη διασφάλιση αυτών των κερδών.

Η ίδρυση του συγκεντρωτισμού είναι μια πραγματικότητα που πρέπει να αντιμετωπίζει κάθε κρυπτογράφηση κατά την εξέλιξή του. Δεν μπορούμε να το αποφύγουμε πλήρως, αλλά τουλάχιστον πρέπει να προσπαθήσουμε να σχεδιάσουμε γύρω από τη σταδιακή αποκέντρωση.

Για το Cardano, σκεφτήκαμε προσεκτικά τι παράγοντες προωθούν τη συγκέντρωση και ποιες τεχνικές θα μπορούσαν να εφαρμοστούν για να ενθαρρύνουμε το πρωτόκολλό μας να γίνει σταδιακά δημόσια υποδομή όπως ο ιστός.

Αναγνωρίζουμε πλήρως ότι η συνολική αποκέντρωση είναι αδύνατη και ίσως ακόμη και αντιπαραγωγική. Ωστόσο, ορισμένοι παράγοντες μπορούν να ενθαρρυνθούν για την παραγωγή ενός πιο ισορροπημένου συστήματος.

Πρώτον, ενώ η κεντρική φύλαξη των κεφαλαίων crowdsale επιτρέπει την ευέλικτη και ταχεία ανάπτυξη του πρωτοκόλλου κατά τις πρώτες μέρες, τελικά η χρηματοδότηση πρέπει να διαφοροποιηθεί και η ταχύτητα ανάπτυξης πρέπει να αποσυρθεί με πιο συστηματικό και σκόπιμο ρυθμό. Με γνώμονα αυτά που είπαμε, η χρηματοδότηση πρέπει να αγνοήσει την πολιτιστική, γλωσσική και γεωγραφική προκατάληψη.

Δεύτερον, καθώς η κοινότητα γίνεται πιο ενημερωμένη για τον υποκείμενο χαρακτήρα της τεχνολογίας κρυπτογράφησης, οι αποφάσεις σχετικά με τον χάρτη πορείας δεν μπορούν να συγκεντρωθούν σε ένα σύνολο βασικών προγραμματιστών ή ιδρυμάτων. Πρέπει να υπάρχει μια μέθοδος βασισμένη σε blockchain για την πρόταση, τον έλεγχο και την εφαρμογή αλλαγών στο πρωτόκολλο.

Τρίτον, τα κίνητρα για τη διατήρηση του blockchain Cardano SL πρέπει να ευθυγραμμιστούν άμεσα με τις συνολικές επιθυμίες όλων των χρηστών. Δεν μπορούμε να επιτρέψουμε να εμφανιστεί μια ομάδα ειδικευμένων ανθρώπων που είναι ανεξάρτητοι από τη βούληση της ευρύτερης κοινότητας.

Για την πρώτη αρχή, επιλέξαμε να ενσωματώσουμε ένα σύστημα ταμείου στο Cardano. Για το δεύτερο, θα αναπτύξουμε μια επίσημη διαδικασία για να προτείνουμε προτάσεις βελτίωσης του Cardano μέσω ενός συστήματος που συντονίζεται από το ίδιο το CSL. Και τρίτον, πιστεύουμε ότι το Ouroboros προσφέρει μια κομψή λύση.

Περισσότερες λεπτομέρειες θα μπορούσαν να δοθούν στα παραπάνω θέματα, αλλά είναι εκτεταμένες από μόνες τους και πέρα από το πεδίο εφαρμογής ενός εγγράφου έρευνας. Ο σχεδιασμός του μηχανισμού είναι ένας από τους πιο περίπλοκους και αλληλοεξαρτώμενους ακαδημαϊκούς τομείς με ελλιπή θεωρία και χωρίς στερεό κανονικό μοντέλο για να σταθεί.

Αντίθετα, η επιστημονική μας προσέγγιση που περιγράφεται στην ενότητα 2 μας εξυπηρετεί καλά εδώ. Η ομάδα Veritas του IOHK συνεργάζεται με μια ομάδα ερευνητών από το Πανεπιστήμιο του Λάνκαστερ υπό την καθοδήγηση του καθηγητή Bingsheng Zhang για την ανάπτυξη του Cardano's reference treasury μοντέλου(μοντέλου θησαυρού αναφοράς του Cardano). Με στόχο την ενσωμάτωση το 2018, αναμένουμε μια ειδική δημοσίευση από ομοτίμους έως τα τέλη του 2017.

Για επίσημη περιγραφή και έλεγχο των αλλαγών σε ένα πρωτόκολλο κρυπτογράφησης, αυτό το θέμα είναι το λιγότερο κατανοητό, καθώς απαιτεί τόσο οντολογικές έννοιες όσο και μηχανισμό για την ενθάρρυνση της ευρείας συμμετοχής. Ίσως θα μπορούσε να προκύψει κάποια μορφή αντιπροσωπευτικής δημοκρατικής διαδικασίας ή η χρήση άμεσων ανατροφοδοτήσεων για την παροχή πιο ορθολογικής ψηφοφορίας.

Αναμένουμε ότι η έρευνα προς αυτή την κατεύθυνση θα καταναλώσει το μεγαλύτερο μέρος της επίσημης συμμετοχής του IOHK στην ανάπτυξη του Cardano. Ως σημείο εκκίνησης, θα αναπτύξουμε παράλληλα με το μοντέλο του ταμείου αναφοράς διάφορους μηχανισμούς για τη λήψη συγκατάθεσης. Απαιτείται περαιτέρω μελέτη για μια οριστική λύση.

Τέλος, οι εργασίες για τη βελτίωση των κινήτρων για το Ouroboros επιβλέπονται από τον καθηγητή Ηλία Κουτσούπια του Πανεπιστημίου της Οξφόρδης. Αφού σταθεροποιηθούν τα κρυπτογραφικά θεμέλια του Ouroboros παράλληλα με όλες τις απαιτούμενες εργασίες κλιμάκωσης, στο πρωτόκολλο αναφοράς θα προστεθεί μια ευρύτερη μελέτη ομολογιών, κυρώσεων και εξωτικών κινήτρων.

Συμπέρασμα

Η κρυπτογράφηση είναι κάτι παραπάνω από το άθροισμα των πρωτοκόλλων της, του πηγαίου κώδικα και του βοηθητικού προγράμματος. Είναι τελικά ένα κοινωνικό σύστημα που εμπνέει, ενεργοποιεί και συνδέει τους ανθρώπους. Απογοητευμένοι από τα πολλά ημίμετρα, τις αποτυχίες και την μη-τήρηση υποσχέσεων προηγούμενων πρωτοκόλλων, ξεκινήσαμε να χτίζουμε κάτι καλύτερο.

Αυτή η διαδικασία δεν είναι απλή ούτε πιστεύαμε ποτέ ότι μπορεί να ολοκληρωθεί. Τα κοινωνικά πρωτόκολλα συνεχίζουν να αλλάζουν επ' αόριστον καθώς οι άνθρωποι και η κοινωνία αλλάζουν. Για να είμαστε χρήσιμοι, θέλουμε να παγιδεύσουμε τη δύναμη της εξέλιξης και να την μεταφέρουμε στο Cardano.

Η εξέλιξη δεν καθοδηγείται από ένα μόνο χέρι ή από ένα μεγάλο σχέδιο. Είναι μια διαδικασία ελευθερίας εμπνευσμένη από ατελείωτα λάθη και προβλήματα. Το Cardano επιδιώκει να είναι η ψηφιακή ενσωμάτωση αυτής της διαδικασίας - αρκετά κατάλληλη για να μπορεί να επιβιώσει στις αγορές του σήμερα και αρκετά προσαρμοσμένη ώστε να εξελιχθεί για να καλύψει τις ανάγκες του μέλλοντος.

Οι προηγούμενες ενότητες αποτυπώνουν μια σύντομη εικόνα για το πώς προσεγγίζουμε αυτόν τον στόχο. Προσπαθήσαμε επιμελώς να αναγνωρίσουμε γνωστικές προκαταλήψεις, να μάθουμε από την ιστορία και να ακολουθήσουμε μια αυστηρή διαδικασία. Προσπαθήσαμε να εξισορροπήσουμε την ανάγκη για ταχεία ανάπτυξη με τυπικές μεθόδους που παραδοσιακά δεν μπορούν να κινηθούν γρήγορα.

Ήταν ένα εξαιρετικό προνόμιο να ξεκινήσουμε αυτό το ταξίδι. Τα τελευταία δύο χρόνια, έχουμε ήδη αναπτύξει μια αποδεδειγμένα ασφαλή απόδειξη πρωτοκόλλου πονταρίσματος, στρατολογήσαμε έναν μικρό στρατό προγραμματιστών Haskell και κάναμε την ανάπτυξη του Cardano την ανησυχία πολλών ταλαντούχων επιστημόνων.

Καθώς προχωρούμε από το εργαστήριο σε ένα ανεπτυγμένο σύστημα στην άγρια φύση, θα υπάρξουν αυξανόμενοι πόνοι, αλλά η ελπίδα μας είναι ότι το μέλλον του Cardano θα μπορούσε να συνοψιστεί σε μία μόνο ανθρωπο-μορφωμένη πρόταση. Το Cardano είναι ένας ρεαλιστής ονειροπόλος που μαθαίνει από τους ηλικιωμένους, είναι καλός πολίτης στην κοινότητά του και βρίσκει πάντα έναν τρόπο να πληρώνει τους λογαριασμούς του.

Δεν μπορούμε να γνωρίζουμε το μέλλον, αλλά είμαστε ευτυχείς που προσπαθούμε να το κάνουμε καλύτερο για όλους. Ευχαριστώ για την ανάγνωση.

Follow our Community to our social media

Telegram: SAPIO Greek Cardano Stake Pool Community	https://t.me/Sapiopool
WebSite	https://sapiopool.com/
Facebook	SapioPool
Twitter	@sapiopool