Hydro Raindrop

Public Authentication On The Blockchain

Ιανουάριος 2018

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

HYDRO: Ετυμολογία – από το αρχαίο Ελληνικό **ύδρο** (*hydro*), που προέρχεται από την λέξη **ύδωρ**.

Το Hydro δίνει τη δυνατότητα σε νέα και προυπάρχοντα ιδιωτικά συστήματα να ενσωματώσουν και να εκμεταλλευτούν με άψογο τρόπο τις αμετάβλητες και διάφανες δυναμικές ενός blockchain, για την ενίσχυση της ασφάλειας των εφαρμογών και των εγγράφων, την διαχείριση ταυτότητας, των συναλλαγών και της τεχνητής νοημοσύνης.

Σε αυτό το έγγραφο, θα γίνει μια αναφορά για τα ιδιωτικά συστήματα, όπως τα APIs, τα οποία θα χρησιμοποιούν το δημόσιο blockchain του Hydro, για την ενίσχυση της ασφάλειας μέσω δημόσιου ελέγχου ταυτότητας (public authentication).

Η προτεινόμενη τεχνολογία ονομάζεται "Raindrop" – μια συναλλαγή που πραγματοποιείται μέσω μιας έξυπνης σύμβασης(smart contract), η οποία επικυρώνει δημοσίως την ιδιωτική πρόσβαση στο σύστημα και μπορεί να συμπληρώσει τις υπάρχουσες μεθόδους ιδιωτικής πιστοποίησης. Η τεχνολογία αποσκοπεί στην παροχή πρόσθετης ασφάλειας για ευαίσθητα οικονομικά δεδομένα τα οποία κινδυνεύουν ολοένα και περισσότερο από την πειρατεία και τις παραβιάσεις.

Η αρχική εφαρμογή του Hydro Raindrop εκτελείται στην πλατφόρμα API του Hydrogen. Αυτή η αρθρωτή δέσμη API διατίθεται σε επιχειρήσεις και προγραμματιστές παγκοσμίως, για να πρωτοτυπήσει, να κατασκευάσει, να δοκιμάσει και να αναπτύξει εξελιγμένες πλατφόρμες και προϊόντα χρηματοοικονομικής τεχνολογίας.

Το Hydro Raindrop θα διατεθεί στην παγκόσμια κοινότητα προγραμματιστών ως λογισμικό ανοιχτού κώδικα (Open source software), ώστε οι προγραμματιστές να μπορούν να ενσωματώσουν το Hydro Raindrop με οποιοδήποτε REST API.

Blockchain & Ethereum

Το Hydro υλοποιείται στο δίκτυο του Ethereum. Πριν από την παροχή περισσότερων λεπτομερειών σχετικά με το έργο, είναι σημαντικό να κατανοήσουμε κάποιες θεμελιώδεις ιδέες για το blockchain και το Ethereum.

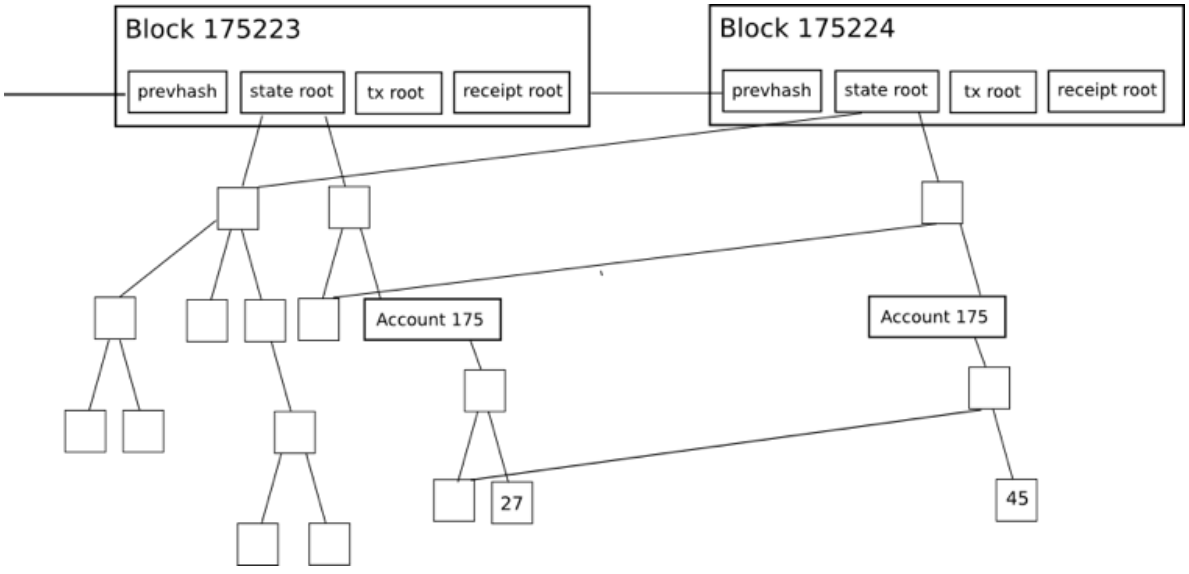
Χτίζοντας στο Ethereum

Όπως εφαρμογές σαν το Snapchat χτίστηκαν με το Swift και άλλα εργαλεία που προσφέρονται από την πλατφόρμα Apple Ios, έτσι και οι εφαρμογές blockchain μπορούν να κατασκευαστούν με βάση το Ethereum. Η Snap Inc δεν χρειάστηκε να κατασκευάσει το Ios, το χρησιμοποίησε ως υποδομή για να ξεκινήσει μια game-changing εφαρμογή κοινωνικών μέσων.

Το Project Hydro είναι παρόμοιο. Στηρίζεται σε χιλιάδες προγραμματιστές παγκοσμίως, οι οποίοι εργάζονται για να κάνουν την υποκείμενη τεχνολογία του blockchain πιο γρήγορη, πιο ισχυρή και πιο αποτελεσματική. Το hydro αξιοποιεί αυτή τη συνεχώς βελτιούμενη υποδομή αναπτύσσοντας αλληλεπιδράσεις επικεντρωμένες στο προϊόν γύρω από την τεχνολογία του blockchain, οι οποίες μπορούν να προσφέρουν αισθητά οφέλη στις εφαρμογές χρηματοπιστωτικών υπηρεσιών.

ΔΕΝΤΡΑ Merkle

Τα δέντρα μερκλ (Merkle Trees) χρησιμοποιούνται σε κατανεμημένα συστήματα για την επαλήθευση δεδομένων (efficient data verification). Είναι αποτελεσματικά, επειδή χρησιμοποιούν τα λεγόμενα hashes αντί για πλήρη αρχεία. Τα hashes είναι τρόποι κωδικοποίησης αρχείων πολύ μικρότερων από το ίδιο το αρχείο. Κάθε block header (κεφαλίδα μπλοκ) στο Ethereum περιέχει τρια δέντρα Merkle για συναλλαγές, έσοδα και καταστάσεις:



Πηγή: Merkling in Ethereum; Vitalik Buterin, Ιδρυτής Ethereum

Αυτό το καθιστά εύκολο για έναν ελαφρύ Client να πάρει επαληθεύσιμες απαντήσεις σε ερωτήματα όπως:

- Υπάρχει αυτός ο λογαριασμός;
- Ποιό είναι το τρέχον υπόλοιπο;
- Έχει συμπεριληφθεί αυτή η συναλλαγή σε ένα συγκεκριμένο block;
- Έχει συμβεί ένα συγκεκριμένο γεγονός σε αυτή τη διεύθυνση σήμερα;

Smart Contracts

Μια βασική δυνατότητα που παρέχει το Ethereum και άλλα δίκτυα που βασίζονται στο blockchain, είναι αυτή των *smart contracts (έξυπνων συμβάσεων). Αυτά είναι αυτο-εκτελέσιμα blocks κώδικα, που μπορούν να αλληλεπιδρούν με πολλαπλά μέρη, αφαιρώντας την ανάγκη για αξιόπιστους μεσάζοντες. Ο κώδικας σε ένα smart contract μπορεί να θεωρηθεί παρόμοιος με τις νομικές ρήτρες ενός συμβόλαιου σε χαρτί, αλλά μπορεί επίσης να επιτύχει περισσότερα λόγω της εκτεταμένης λειτουργικότητας. Οι συμβάσεις αυτές μπορούν να έχουν κανόνες, προϋποθέσεις και κυρώσεις για την μη τήρηση των κανόνων ή να ξεκινήσουν άλλες διαδικασίες. Όταν ενεργοποιούνται, εκτελούνται όπως αναφέρθηκε αρχικά κατά την εγκατάσταση τους στο public chain, προσφέροντας ενσωματωμένα στοιχεία, τα οποία είναι αμετάβλητα και αποκεντρωμένα (decentralized).*

Τα smart contracts είναι ένα σημαντικό εργαλείο για την οικοδόμηση στην υποδομή του Ethereum. Η βασική λειτουργικότητα του Hydro blockchain layer επιτυγχάνεται μέσω προσαρμοσμένων συμβάσεων, όπως αναλύεται αργότερα σε αυτό το άρθρο.

Εικονική μηχανή Ethereum

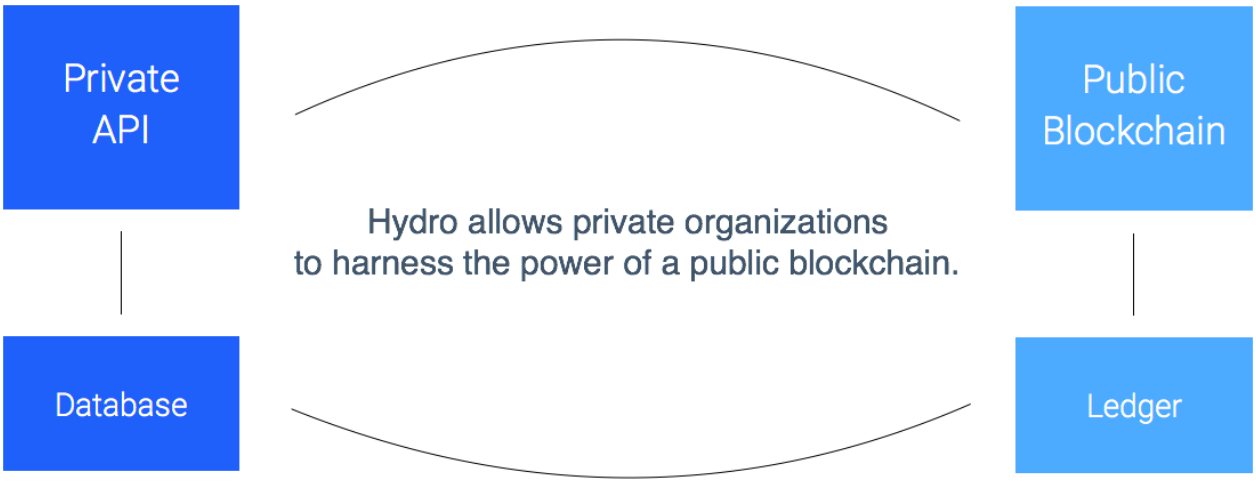
Η εικονική μηχανή Ethereum ή αλλιώς Ethereum Virtual Machine (EVM) είναι το περιβάλλον εκτέλεσης για τα smart contracts στο Ethereum. Το EVM συμβάλλει στην αποτροπή επιθέσεων Denial of Service (DoS), διασφαλίζει ότι τα προγράμματα παραμένουν ανεπηρέαστα και επιτρέπει την αδιάκοπη επικοινωνία. Οι ενέργειες σχετικά με την EVM έχουν ένα κόστος το οποίο σχετίζεται με αυτές, ονομαζόμενο gas, το οποίο εξαρτάται από τους απαιτούμενους υπολογιστικούς πόρους που θα χρειαστούν. Κάθε συναλλαγή έχει μια μέγιστη ποσότητα gas που μπορεί να χρησιμοποιηθεί, η οποία ονομάζεται gas limit. Αν το gas που θα καταναλωθεί από μια συναλλαγή φτάσει στο όριο, διακόπτει την διαδικασία.

Public Ledger

Public Ledger για ιδιωτικά συστήματα

Τα συστήματα που διαχειρίζονται πλατφόρμες οικονομικών υπηρεσιών, ιστοσελίδες και εφαρμογές, συχνά μπορούν να περιγραφούν ως μέσα ροής δεδομένων – στέλνουν, δέχονται, αποθηκεύουν, αναβαθμίζουν και επεξεργάζονται δεδομένα για τα πρόσωπα με τα οποία αλληλεπιδρούν. Εξαιτίας της φύσης αυτών των δεδομένων και των χρηματοπιστωτικών υπηρεσιών γενικότερα, τα συστήματα αυτά, συχνά φιλοξενούν πολύπλοκες λειτουργίες με έναν ιδιωτικό και συγκεντρωτικό τρόπο. Η εμπιστοσύνη σε ιδιωτικές δομές με τη σειρά της, ανοίγει την πόρτα σε μια ποικιλία από ασφάλειες, διαφάνεια, καθώς και σε κέρδη αποδοτικότητας, με στόχο να τα υιοθετηθούν ενσωματώνοντας εξωτερικές δυνάμεις, που θα υπερβαίνουν την έκταση του εσωτερικού συστήματος.

Αυτό συμβαίνει με την πλατφόρμα API του Hydro. Το Hydro επιδιώκει να αξιοποιήσει τα προαναφερθέντα οφέλη, επιτρέποντας στους χρήστες του Hydro να αλληλεπιδρούν με ένα blockchain με τρόπους που ενσωματώνονται απρόσκοπτα στο θεμελιώδες ιδιωτικό οικοσύστημα του Hydro.

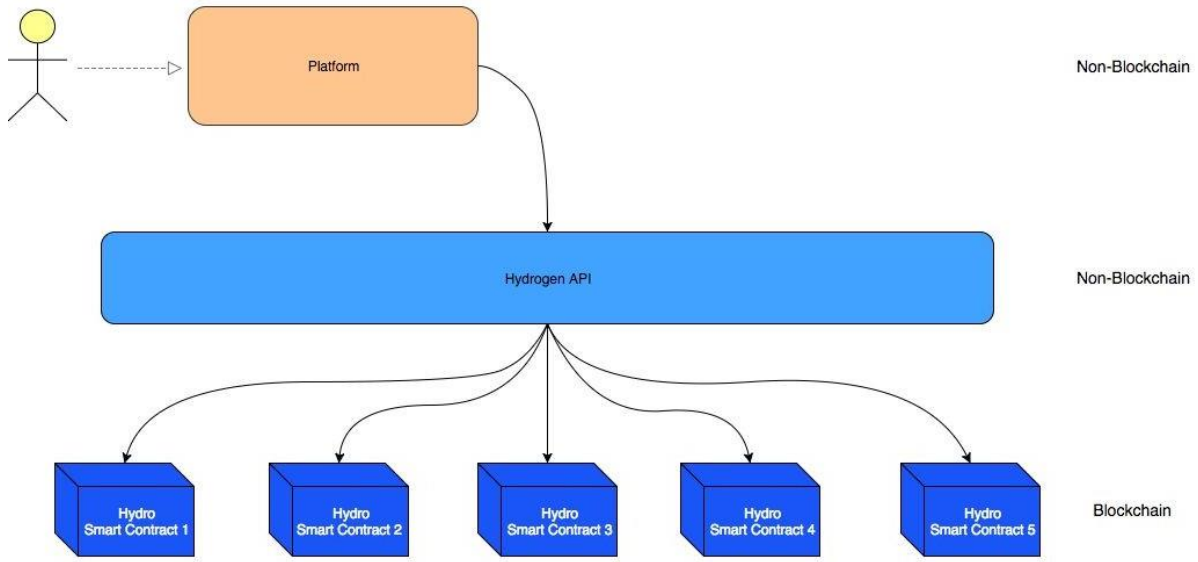


Οι δημόσιες λειτουργίες βασισμένες στο blockchain μπορούν να πραγματοποιηθούν πριν, κατα την διάρκεια ή μετά από τις ιδιωτικές λειτουργίες. Η αλληλεπίδραση μεταξύ ιδιωτικών και δημόσιων στοιχείων μπορεί να χρησιμεύσει για την επικύρωση, τη σφράγιση, την καταγραφή ή την ενίσχυση διαδικασιών εντός ενός οικοσυστήματος.

Το ήθος αυτού του μοντέλου καθιστά τις διαδικασίες πιο εύρωστες αξιοποιώντας τα οφέλη της τεχνολογίας του blockchain, ειδικά εκεί, όπου μπορεί να παράγει τις πιο θετικές επιπτώσεις. Ενώ αυτή η υβριδική δομή μπορεί να μην ισχύει για όλες τις πλατφόρμες, το Hydro επικεντρώνεται στην παροχή αξίας για τις περιπτώσεις στις οποίες ισχύει.

Αρχιτεκτονική Πρότυπο

Το Hydro διαφέρει από πολλές υπάρχουσες πρωτοβουλίες blockchain, διότι μπορεί να υπάρχει ανεξάρτητα και να τοποθετείται γύρω από νέα ή προϋπάρχοντα συστήματα χωρίς να απαιτείται συστηματική αλλαγή. Αντί να αντικαταστήσει, το Hydro επιδιώκει να βελτιώσει. Οι πλατφόρμες και τα ιδρύματα που συνδέονται με το Hydrogen API μπορούν να έχουν αυτόματη πρόσβαση στο blockchain.



Το εύρος των πλατφορμών χρηματοπιστωτικών υπηρεσιών που μπορούν να αξιοποιήσουν το Hydrogen είναι ευρύ. Αυτές οι πλατφόρμες μπορούν να τροφοδοτήσουν σχεδόν οποιαδήποτε εμπειρία, να φιλοξενήσουν οποιοδήποτε αριθμό ιδιόκτητων υπηρεσιών, να εκτελέσουν οποιαδήποτε λειτουργία ιδιωτικών δεδομένων και να αναπτυχθούν σε οποιοδήποτε περιβάλλον. Αυτό επιτυγχάνεται με τη δομική προσαρμογή του Hydrogen και συνεργάζεται με το Hydro, ενεργώντας ως συμπληρωματικός οδηγός υιοθεσίας.

Raindrop

Χτισμένο στο public ledger του Hydro υπάρχει μια υπηρεσία ελέγχου ταυτότητας βασισμένη στο blockchain, που ονομάζεται "Raindrop". Αυτό προσφέρει μια ξεχωριστή, αμετάβλητη, παγκοσμίως εμφανή στρώση ασφάλειας που επαληθεύει αν μια αίτηση πρόσβασης προέρχεται από μια εγκεκριμένη πηγή.

Τα ιδιωτικά πρωτόκολλα ελέγχου ταυτότητα όπως το OAuth 2.0 προσφέρουν διαφορετικά επίπεδα ευρωστίας και χρησιμότητας για το φάσμα των περιπτώσεων χρήσης που υπάρχουν. Υπάρχει μικρή ανάγκη να ανταγωνιστεί ή να προσπαθήσει να αντικαταστήσει αυτά τα πρωτόκολλα. Το Hydro προσφέρει έναν τρόπο να τα ενισχύσει με την ενσωμάτωση των μηχανισμών του blockchain ως συστατικό της διαδικασίας ελέγχου ταυτότητας. Αυτό μπορεί να προσθέσει ένα χρήσιμο στρώμα ασφάλειας για να βοηθήσει στην αποτροπή παραβιάσεων του συστήματος και την διαρροή εμπιστευτικών πληροφοριών.

Πριν εξετάσουμε την τεχνική όψη του Raindrop, θα ρίξουμε μια ματιά στο πρόβλημα που που προσπαθεί να λύσει.

Η Κατάσταση της Χρηματοοικονιμικής Ασφάλειας

Η έγερση της εποχής των δεδομένων (data age), έφερε μαζί της την τρωτότητα στα συστήματα, και αυτό είναι ιδιαίτερα σημαντικό για τις χρηματοπιστωτικές υπηρεσίες. Οι χρηματοπιστωτικές πλατφόρμες μπορούν να θεωρηθούν ως πύλες προς μεγάλο αριθμό ιδιωτικών και ευαίσθητων δεδομένων, όπως είναι οι αριθμοί ταυτότητας, τα διαπισπευτήρια λογαριασμών και τα ιστορικά των συναλλαγών. Εξαιτίας της σημαντικότητας των δεδομένων ταυτοποίησης, η πρόσβαση σε αυτά από ανεπιθύμητες πηγές, ακολλουθείτε συχνά από καταστροφικά αποτελέσματα.

Η εταιρία ερευνών Trend Micro δημοσίευσε μια αναφορά στην οποία αναφέρει ότι τα κλεμμένα στοιχεία προσωπικής ταυτοποίησης τα οποία αναφέρονται ως Personally Identifiable Information (PII), πωλούνται στο Deep Web για μόλις $1, οι σαρώσεις εγγράφων όπως τα διαβατήρια είναι διαθέσιμα για μόλις $10 και τα διαπισπευτήρια σύνδεσης σε λογαριασμούς τραπέζης μόλις $200, καθιστώντας την κατανομή των κλεμμένων δεδομένων ευκόλως προσβάσιμη.

Ωστόσο, το υφιστάμενο χρηματοπιστωτικό σύστημα δεν έχει πεντακάθαρο ιστορικό όταν πρόκειται για την πρόληψη, την διάγνωση κα την επικοινωνία για τις παραβιάσεις δεδομένων με τους μετόχους.

- Σύμφωνα με πρόσφατη μελέτη της Javelin Strategy & Research με τίτλο – *The 2017 Identity Fraud Study* – $16 δισεκατομμύρια δολάρια κλάπηκαν από 15,4 εκατομμύρια καταναλωτές από τις Η.Π.Α. το 2016 λόγω αποτυχιών του χρηματοπιστωτικού συστήματος για την προστασία προσωπικών στοιχείων (των PII).

- Τον Απρίλιο του 2017, η Symantec δημοσίευσε την αναφορά *Internet Security Threat Report*, η οποία εκτιμά ότι κατα τη διάρκεια του 2016, διατέθηκαν 1,1 δισεκατομμύρια αρχεία PII σε διάφορες πηγές.

- Στο άρθρο *2016 Year End Data Breach Quickview* από την Risk Based Security, διαπιστώθηκε ότι το 2016 σημειώθηκαν 4,149 παραβιάσεις δεδομένων σε επιχειρήσεις παγκοσμίως, εκθέτοντας πάνω από 4,2 δις αρχεία.

- Στο *2017 Thales Data Threat Report – Financial Services Edition*, μια έρευνα των global IT professionals στον τομέα των επαγγελματικών υπηρεσιών, διαπίστωσε ότι το 49% των οργανισμών χρηματοπιστωτικών υπηρεσιών υπέστησαν παραβίαση ασφαλείας στο παρελθόν, το 78% δαπανούν περισσότερα για να προστατεύσουν τον εαυτό τους αλλά το 73% ξεκινά νέες πρωτοβουλίες που σχετίζονται με το AI, το IoT και τα τις τεχνολογίες cloud πριν προετοιμάσουν τις κατάλληλες λύσεις ασφάλειας.

Equifax Breach

Στις 29 Ιουλίου 2017, η Equifax, μια 118ετής αμερικάνικη υπηρεσία παροχής στοιχείων πιστοληπτικής αναφοράς, έπεσε θύμα hacking με αποτέλεσμα 143 εκατομμύρια PII χρηστών να εκτεθούν, συμπεριλαμβανομένων και των αριθμών κοινωνικής ασφάλισης, καθώς τα στοιχεία πιστωτικών καρτών 209.000 πελατών είχαν παραβιαστεί.

Ποια ήταν η αιτία αυτής της παραβίασης;

Εεκίνησε με μια από τις τεχνολογίες backend που χρησιμοποιεί η Equifax. Το Struts είναι ένα open source framework για την ανάπτυξη web εφαρμογών στη γλώσσα προγραμματισμού Java, η οποία δημιουργήθηκε από την Apache Software Foundation. Το CVE-2017-9805 είναι ένα τρωτό σημείο στα Apache Struts σχετικά με τη χρήση του plugin Struts REST με το XStream handler για να χειριστεί τα φορτία XML. Αν παραβιαστεί, επιτρέπει στον "εισβολέα" να εκτελέσει κακόβουλο κώδικα στον διακοσμιστή της εφαρμογής, είτε για να αναλάβει τη μηχανή, είτε για να εκκινήσει περαιτέρω επιθέσεις από αυτήν. Αυτό ήταν patched από την Apache δύο μήνες πριν από την παραβίαση της Equifax.

Το Apache Struts περιέχει ένα ελάττωμα στο XStream Plugin REST το οποίο ενεργοποιείται καθώς το πρόγραμμα αποσειριοποιεί την παρεχόμενη από τον χρήστη είσοδο σε αιτήσεις XML. Συγκεκριμένα, το πρόβλημα παρουσιάζεται στη μέθοδο toObject() της XStreamHandler, η οποία δεν επιβάλλει περιορισμούς στην εισερχόμενη τιμή όταν χρησιμοποιεί αποσειριοποίηση XStream σε ένα αντικείμενο, με αποτέλεσμα την ύπαρξη αυθαίρετων τρωτών σημείων εκτέλεσης κώδικα.

Ακόμα και αν το plugin REST ήταν εκτεθειμένο, θα είχε σημασία; Υπάρχει τρόπος να χρημιμοποιηθεί η τεχνολογία του blockchain για να εξασφαλιστούν οι οικονομικές πληροφορίες των 143 εκκατομυρίων πελατών, ενώ εξακολουθούν να βασίζονται σε υπάρχοντα συστήματα REST API και Java;

Προσθέτοντας ένα Blockchain Layer

Είναι σαφές ότι η ακεραιότητα των πυλών χρηματοοικονομικών δεδομένων μπορεί να βελτιωθεί.

Ας εξετάσουμε πως μπορεί να επιτευχθεί ένα επιπλέον επίπεδο ασφάλειας μέσω του Hydro.

Οι θεμελιώδεις μηχανισμοί συναίνεσης του δικτύου Ethereum διασφαλίζουν την εγκυρότητα των συναλλαγών, διότι οι συμμετέχοντες συλλογικά επεξεργάζονται συναλλαγές που έχουν υπογραφεί σωστά. Αυτή η πραγματικότητα οδηγεί στο decentralization και την σταθερότητα, αλλά κυρίως, παρέχει ένα διάνυσμα για τον μετριασμό της μη εξουσιοδοτημένης πρόσβασης σε μια πύλη που χειρίζεται ευαίσθητα δεδομένα.

Με το Hydro, ο έλεγχος ταυτότητας μπορεί να εξαρτηθεί από τις πράξεις συναλλαγής στο blockchain. Ένα API για παράδειγμα, μπορεί να επιλέξει να επικυρώσει τους προγραμματιστές και τις εφαρμογές, απαιτώντας από αυτούς να ξεκινήσουν συγκεκριμένες συναλλαγές με ιδιαίτερο φορτίο δεδομένων, μεταξύ συγκεκριμένων διευθύνσεων στο blockchain, ως προϋπόθεση ότι ξεκινά ένα πρωτόκολλο ελέγχου ταυτότητας.

Το Hydro Raindrop

Το Rain (“βροχή”) περιέχει πακέτα συμπυκνωμένου νερού που κυμαίνονται από 0,0001 έως 0,005 εκατοστά σε διάμετρο. Σε μια τυπική καταιγίδα, υπάρχουν δισεκατομμύρια από αυτά τα πακέτα, το καθένα με τυχαίο μέγεθος, ταχύτητα και σχήμα. Εξαιτίας αυτού, δεν μπορεί κανείς να προβλέψει με ακρίβεια την ακριβή φύση της βροχής. Ομοίως, κάθε συναλλαγή ελέγχου ταυτότητας του Hydro είναι μοναδική και πρακτικά αδύνατη να συμβεί τυχαία - γι 'αυτό τα αποκαλούμε Raindrops.

Οι πλατφόρμες χρηματοπιστωτικών υπηρεσιών χρησιμοποιούν συνήθως την επαλήθευση μέσω των μικροκαταθέσεων για την επικύρωση των λογαριασμών πελατών. Η ιδέα είναι απλή: η πλατφόρμα δημιουργεί μικρές καταθέσεις τυχαίων ποσών σε τραπεζικούς λογαριασμούς που δηλώνουν οι χρήστες. Προκειμένου να αποδειχθεί ότι ο χρήστης πράγματι κατέχει τον εν λόγω λογαριασμό, αυτός πρέπει να μεταφέρει τα ποσά των καταθέσεων πίσω στην πλατφόρμα, τα οποία στη συνέχεια επικυρώνονται. Ο μόνος τρόπος με τον οποίο ο χρήστης μπορεί να γνωρίζει τα έγκυρα ποσά (εκτός από το να μαντέψει) είναι η πρόσβαση στους εν λόγω τραπεζικούς λογαριασμούς.

Η επαλήθευση βάσει του Raindrop με το Hydro είναι ανάλογη. Αντί να στέλνουμε στον χρήστη ένα ποσό και να το αναμεταδίδουμε, ορίζουμε μια συναλλαγή και ο χρήστης πρέπει να το εκτελέσει από ένα γνωστό πορτοφόλι. Ο μόνος τρόπος με τον οποίο ο χρήστης μπορεί να πραγματοποιήσει μια έγκυρη συναλλαγή είναι η πρόσβαση στο εν λόγω πορτοφόλι.

Χρησιμοποιώντας τα Raindrops, τόσο το σύστημα όσο και το accessor μπορούν να παρακολουθούν τις προσπάθειες εξουσιοδότησης σε ένα αμετάβλητο public ledger. Αυτή η βασισμένη σε blockchain συναλλαγή, αποσυνδέεται από τις βασικές λειτουργίες του συστήματος, εμφανίζεται σε ένα κατανεμημένο δίκτυο και εξαρτάται από την ιδιοκτησία των private keys. Επομένως, χρησιμεύει ως χρήσιμο στοιχείο επικύρωσης.

Μια Προσεκτική Ματιά

Υπάρχουν τέσσερα στοιχεία που συμμετέχουν στη διαδικασία ελέγχου ταυτότητας του Hydro:

1. *Accessor* - Η ομάδα επιδιώκει να αποκτήσει πρόσβαση σε ενα συστημα. Στην περίπτωση του Hydrogen, ο accessor είναι ένα χηματοπιστωτικο ίδρυμα ή μια εφαρμογή που χρησιμοποιεί τα Hydrogen APIs για την βασική ψηφιακη του υποδομή.
2. *System* - Το σύστημα(*System*) ή η πύλη στην οποία έχει πρόσβαση ο Accessor. Για το Hydrogen, το *System* είναι το ίδιο το Hydrogen API.
3. *Hydro* - Η ενότητα που χρησιμοποιείται από το *System* για την επικοινωνία και τη διασύνδεση με το blockchain.
4. *Blockchain* – Το κατανεμημένο public ledger που επεξεργάζεται τις συναλλαγές HYDRO και περιέχει τα Hydro smart contracts, μέσω των οποίων πληροφορίες μπορούν να εισαχθούν, να ληφθούν ή να λειτουργήσουν σε αυτά.

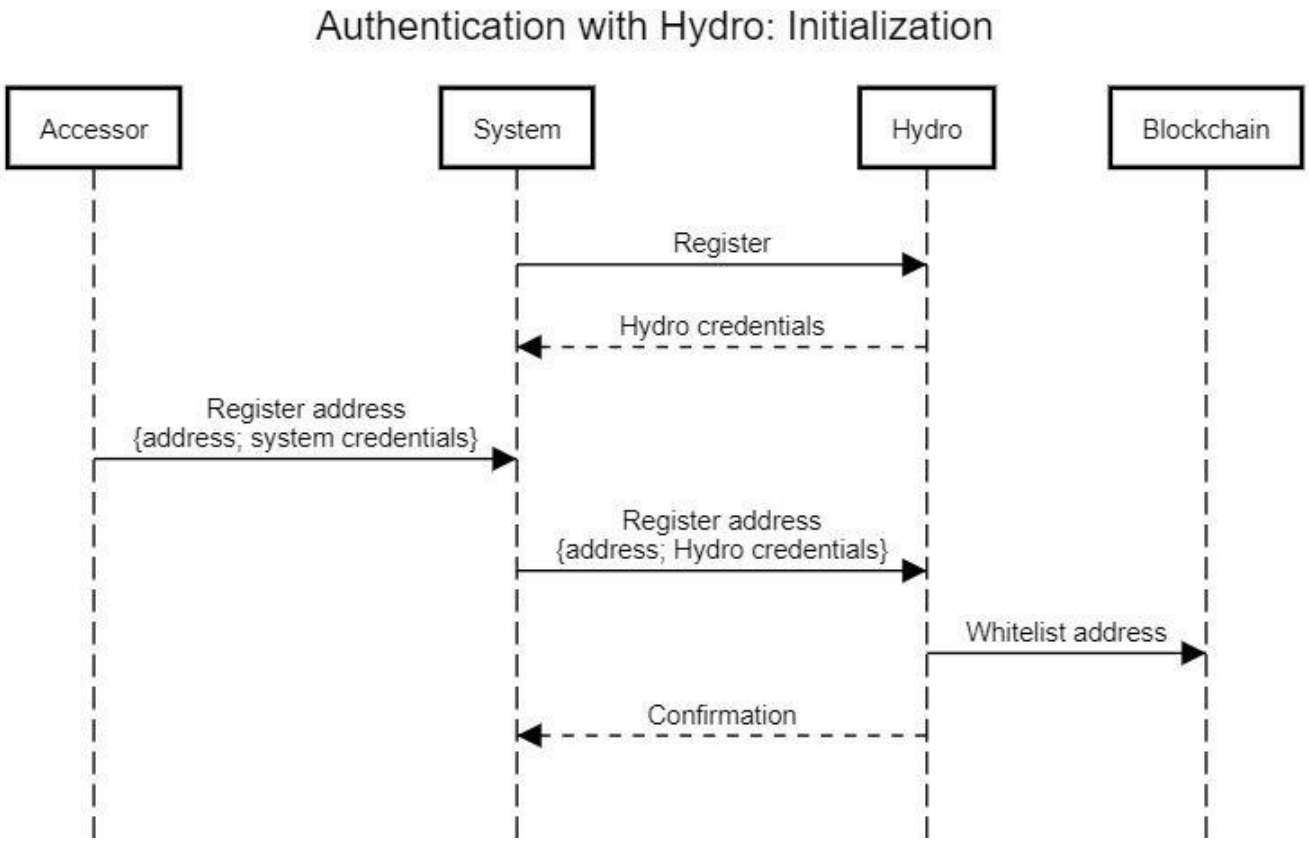
Κάθε Raindrop, αποτελείται από ένα σύνολο πέντε παραμέτρων συναλλαγών:

1. *Sender* - Η διεύθυνση που πρέπει να ξεκινήσει τη συναλλαγή.
2. *Receiver* - Ο προορισμός της συναλλαγής. Αυτό αντιστοιχεί στην κλήση μιας μεθόδου σε ένα Hydro smart contract.
3. *ID* - Ένα αναγνωριστικό που συνδέεται με το Σύστημα.
4. *Quantity* - Ένας ακριβής αριθμός HYDRO που επιλέχθηκε για αποστολή.
5. *Challenge* - Μια τυχαία παραγόμενη αλφαριθμητική σειρά.

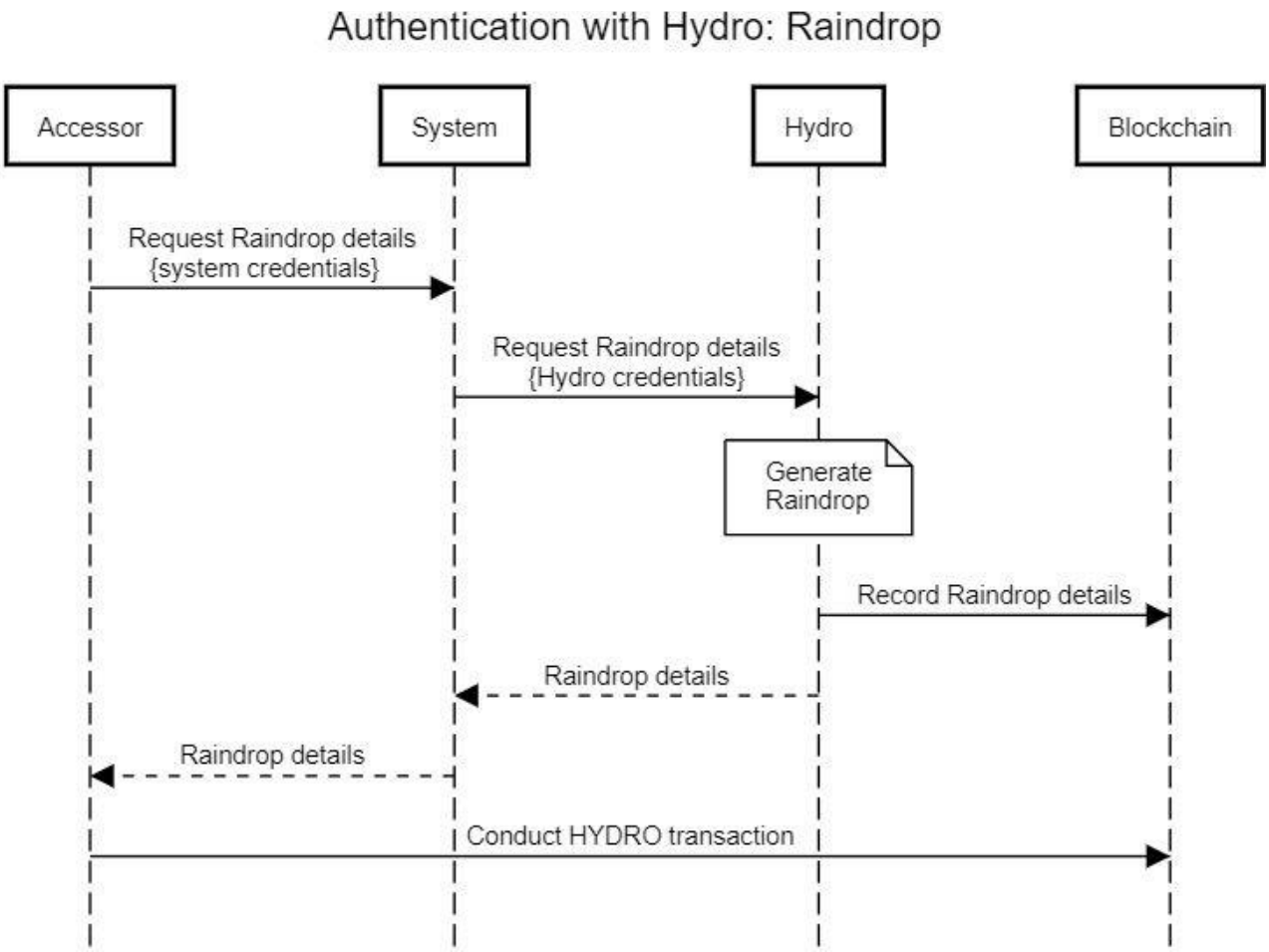
Παρακάτω υπάρχει μια περίληψη της διαδικασίας επαλήθευσης ταυτότητας, η οποία μπορεί γενικά να ταξινομηθεί σε τρία στάδια:

1. Initialization (Αρχικοποίηση)
2. Raindrop
3. Validation (Επικύρωση)

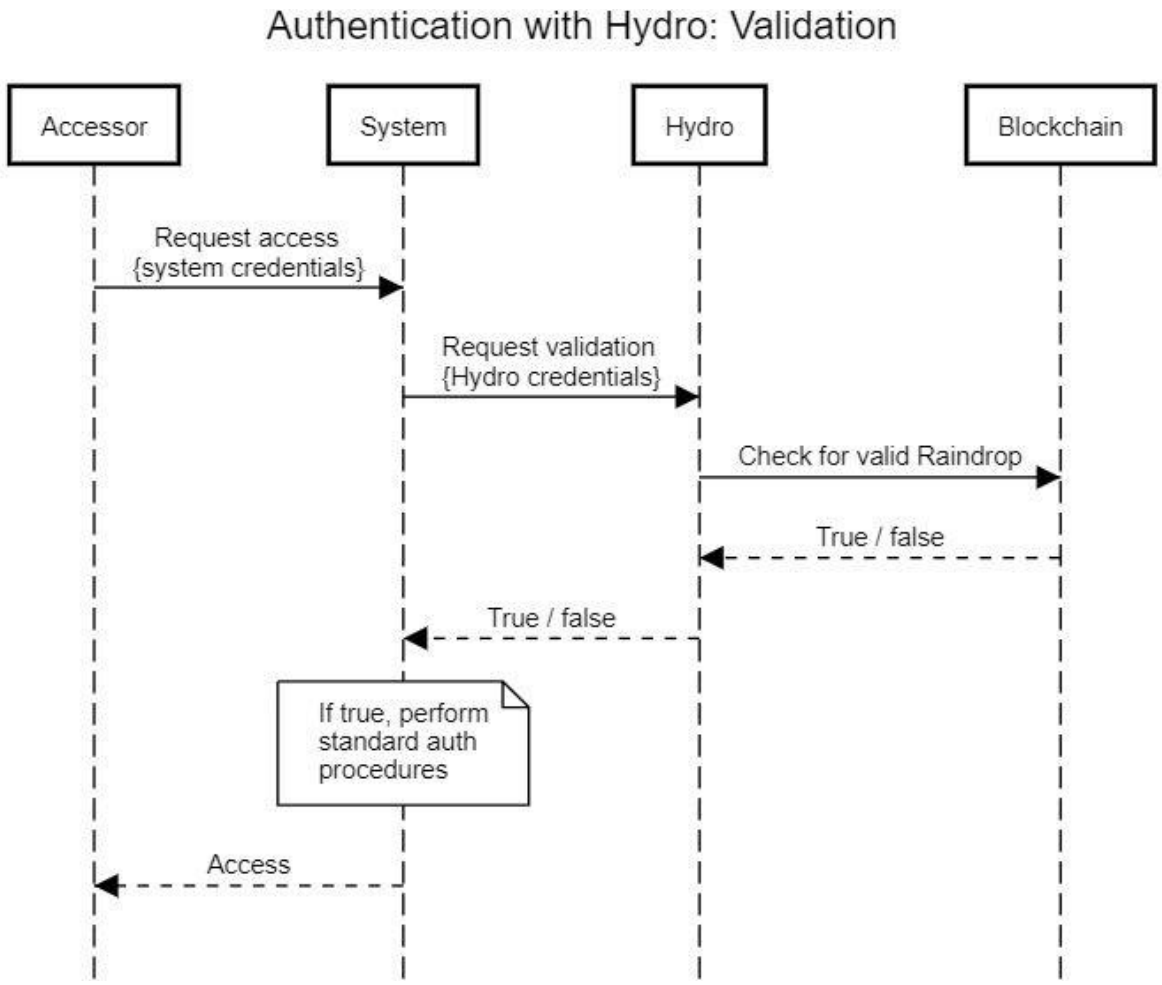
Η αρχικοποίηση ξεκινά με ένα σύστημα (π.χ. Hydrogen), καταχωρημένο για να χρησιμοποιήσει το Hydro και να λαμβάνει πιστοποιητικά, επιτρέποντας στο σύστημα να επικοινωνεί με το blockchain μέσω της μονάδας Hydro. Το Σύστημα παρακολουθεί ένα Accessor (π.χ. ένα χρηματοπιστωτικό ίδρυμα) που καταχωρεί ένα public ledger και στη συνέχεια διαβιβάζει την καταχωρημένη διεύθυνση στο Hydro. Αυτή η διεύθυνση γράφεται αμετάβλητη στο blockchain, σε ένα whitelist το οποίο είναι αποθηκευμένο σε ένα Hydro smart contract. Το Σύστημα λαμβάνει μια επιβεβαίωση ότι η διεύθυνση ήταν whitelisted, η οποία μπορεί επίσης να επαληθευτεί μέσω της δημόσιας προβολής. Η καταχώριση του συστήματος πρέπει να πραγματοποιείται μόνο μία φορά, ενώ το Accessor whitelisting πρέπει να εμφανίζεται μόνο μία φορά ανά Accessor.



Μετά την ολοκλήρωση της αρχικοποίησης, μπορεί να ξεκινήσει ο πυρήνας της διαδικασίας ελέγχου ταυτότητας Hydro. Ο Accessor, ο οποίος πρέπει να εκτελέσει μια συναλλαγή Raindrop, ξεκινάει αυτή τη διαδικασία ζητώντας λεπτομέρειες του Raindrop από το Σύστημα και το Σύστημα μεταφέρει το αίτημα στο Hydro. Το Hydro δημιουργεί ένα νέο Raindrop, αποθηκεύει συγκεκριμένες λεπτομέρειες αμετάβλητες στο blockchain και επιστρέφει όλες τις λεπτομέρειες στο Accessor μέσω του συστήματος. Ο Accessor, εφοδιασμένος με όλες τις απαιτούμενες πληροφορίες, πραγματοποιεί μια συναλλαγή από την καταχωρημένη διεύθυνση σε μια μέθοδο στο Hydro smart contract. Εάν η διεύθυνση δεν είναι whitelisted, η ενέργεια απορρίπτεται - διαφορετικά, καταγράφεται στο smart contract. Είναι σημαντικό να σημειωθεί ότι αυτή η συναλλαγή θα πρέπει να πραγματοποιηθεί εκτός του Συστήματος, απευθείας από τον Accessor στο Blockchain, καθώς πρέπει να υπογραφεί με το private key του Accessor (το οποίο θα μπορεί να αποκτήσει μόνο ο Accessor).



Το τελικό βήμα της διαδικασίας είναι η Επικύρωση. Σε αυτό το βήμα, ο Accessor ζητά πρόσβαση στο Σύστημα μέσω του εγκατεστημένου μηχανισμού του συστήματος. Πριν από την εφαρμογή οποιουδήποτε από τα πρότυπα πρωτόκολλα ελέγχου ταυτότητας, το Σύστημα ζητά από το Hydro, αν ο Accessor έχει πραγματοποιήσει ή όχι μια έγκυρη συναλλαγή Raindrop. Το Hydro συνεργάζεται με το smart contract, ελέγχει την εγκυρότητα και ανταποκρίνεται με αληθή / ψευδή προσδιορισμό. Το Σύστημα είναι σε θέση να αποφασίσει πώς θα πρέπει να προχωρήσει βάσει αυτού του προσδιορισμού - εάν είναι false (ψευδές), το Σύστημα μπορεί να αρνηθεί την πρόσβαση, και αν είναι true (αληθές), το Σύστημα μπορεί να δώσει πρόσβαση.



Αν λάβουμε υπ' όψιν τα βασικά διαπιστευτήρια του συστήματος ή το υπάρχον πρωτόκολλο συστήματος που είναι στη θέση του, ως έναν παράγοντα επαλήθευσης της ταυτότητας, είναι σημαντικό το Hydro να προσφέρει και έναν δεύτερο παράγοντα. Με την εξέταση των δύο πρωταρχικών φορέων επίθεσης, μπορούμε να επιβεβαιώσουμε άμεσα τη χρησιμότητά του:

- Φορέας 1 - Ο Attacker κλέβει τα διαπιστευτήρια του συστήματος του Accessor
  - Ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση στο σύστημα με έγκυρα διαπιστευτήρια συστήματος
  - Το Σύστημα ελέγχει με το Hydro για να διαπιστώσει αν υπήρξε έγκυρη συναλλαγή στο blockchain
  - Το Hydro επιστρέφει false, και το σύστημα αρνείται την πρόσβαση
- Φορέας 2 – Ο Attacker κλέβει το private key από το πορτοφόλι του Accesser
  - Ο Attacker προσπαθεί να διεξάγει μια συναλλαγή Hydro από την καταχωρημένη διεύθυνση, χωρίς να χρειάζεται λεπτομέρειες Raindrop
  - Ο Attacker δεν μπορεί να κάνει μια έγκυρη συναλλαγή στο blockchain

- Ο Attacker επίσης δεν μπορεί να ζητήσει πρόσβαση στο σύστημα χωρίς τα κατάλληλα διαπισπευτήρια του συστήματος

Είναι σαφές ότι ο Attacker πρέπει να κλέψει και τα δύο βασικά διαπιστευτήρια συστήματος και το ιδιωτικό κλειδί πορτοφολιού του Accessor για να αποκτήσει πρόσβαση στο σύστημα. Από αυτή την άποψη, το Hydro προσέθεσε με επιτυχία έναν επιπλέον παράγοντα επαλήθευσης ταυτότητας.

Διάθεση του Raindrop στο Κοινό

Παρόλο που αυτή η βασισμένη στο blockchain υπηρεσία ελέγχου ταυτότητας σχεδιάστηκε για να διασφαλίσει το οικοσύστημα API του Hydrogen, είναι ευρέως εφαρμόσιμη σε διαφορετικές πλατφόρμες και συστήματα. Επειδή και άλλοι μπορούν να επωφεληθούν από αυτό το επίπεδο επαλήθευσης και ασφάλειας, διατίθεται ανοιχτό για χρήση.

Ακριβώς όπως το Hydrogen θα το ενσωματώσει ως προϋπόθεση για την πρόσβαση στο οικοσύστημα του API, το ίδιο μπορεί και οποιοδήποτε άλλο σύστημα να το προσθέσει σε υπάρχουσες διαδικασίες και πρωτόκολλα. Κάθε πλατφόρμα είτε πρόκειται για API, εφαρμογή, λογισμικό επιχείρησης, πλατφόρμα παιχνιδιών κ.λπ., μπορεί να χρησιμοποιήσει το Hydro για σκοπούς επαλήθευσης ταυτότητας. Το έγγραφο θα είναι διαθέσιμο στο GitHub για όσους επιθυμούν να ενσωματώσουν αυτό το επίπεδο του blockchain σε ένα πλαίσιο ελέγχου ταυτότητας ή API REST.

Case Study – Raindrop With OAuth 2.0

Υπάρχουν δεκάδες τρόποι με τους οποίους το Raindrop μπορεί να χρησιμοποιηθεί από ιδιωτικούς οργανισμούς. Τα ιδιωτικά API, οι βάσεις δεδομένων και τα δίκτυα έχουν δημιουργήσει επεξεργασμένα συστήματα με tokens, κλειδιά, εφαρμογές και πρωτόκολλα κατά την τελευταία δεκαετία, σε μια προσπάθεια να εξασφαλίσουν τα ευαίσθητα δεδομένα. Η Google για παράδειγμα, έγινε ένας από τους πιο δημοφιλείς προμηθευτές προϊόντων στην αγορά με την εφαρμογή Google Authenticator. Όπως αναφέρθηκε προηγουμένως, δεν υπάρχει κανένας λόγος να ανταγωνιστεί ή να αντικαταστήσει κανείς αυτά τα υπάρχοντα πρωτόκολλα.

Ως μελέτη περίπτωσης (Case Study), παρουσιάζεται μια σύντομη επισκόπηση του τρόπου με τον οποίο το Hydrogen εφαρμόζει την πιστοποίηση Hydro ως επίπεδο ασφαλείας στο συνολικό πλαίσιο ασφαλείας του API:

1. Οι έταιροι του Hydrogen API θα πρέπει πρωτίστως να έχουν τις διευθύνσεις IP των διαφόρων περιβαλλόντων τους whitelisted.
2. Οι έταιροι θα πρέπει να κάνουν αίτηση για να γίνει whitelist μια διεύθυνση Hydro.
3. Όλες οι κλήσεις προς τα Hydrogen APIs και οι μεταφορές δεδομένων είναι κρυπτογραφημένες και μεταδίδονται μέσω του πρωτοκόλλου HTTPS.
4. Οι έταιροι πρέπει να ολοκληρώσουν μια έγκυρη συναλλαγή Hydro raindrop από την καταχωρημένη διεύθυνση Hydro.

5. Οι έταιροι θα πρέπει να χρησιμοποιούν την επικύρωση OAuth 2.0. Το OAuth 2.0 (Open Authorization) είναι ένα ανοικτό πρότυπο για τον έλεγχο ταυτότητας και την εξουσιοδότηση βάσει token. Το Hydrogen υποστηρίζει τους τύπους χορήγησης "Πιστοποιητικά κωδικού πρόσβασης ιδιοκτήτη" και "Πιστοποιητικά πελάτη", και κάθε χρήστης API πρέπει να παράσχει διαπιστευτήρια για αίτημα ελέγχου ταυτότητας.
6. Εάν κανένα από τα πέντε παραπάνω στοιχεία δεν παραβιαστεί, ο έταιρος του Hydrogen διαθέτει ένα μοναδικό token, το οποίο πρέπει να ελεγχθεί και να επαληθεύεται με κάθε κλήση API.
7. Το token ισχύει για 24 ώρες, μετά τις 24 ώρες ο έταιρος θα πρέπει να επικυρωθεί και πάλι.

Εάν κάποιο από αυτά τα βήματα παραβιαστεί, ο χρήστης είναι άμεσα κλειδωμένος από την πρόσβαση API. Ένας χάκερ δεν μπορεί να παρακάμψει αυτούς τους παράγοντες ασφάλειας υποθέτοντας τυχαία, επειδή υπάρχουν τρισεκατομμύρια μοναδικοί συνδυασμοί.

Ο έλεγχος ταυτότητας βασιζόμενος στο Hydro blockchain είναι ένα σημαντικό στοιχείο του πρωτοκόλλου ασφάλειας του Hydrogen. Η ομάδα του Hydrogen ενθαρρύνει τους συνεργάτες της να δημιουργήσουν πορτοφόλια πολλαπλών υπογραφών (multi-signature wallets) και την αποθήκευση των ιδιωτικών κλειδιών τους σε πολλές ασφαλείς τοποθεσίες ανεξάρτητα από τα άλλα διαπιστευτήρια, ώστε να μην υπάρχει κανένα τρωτό σημείο. Ένα πορτοφόλι πολλαπλών υπογραφών που είναι σωστά ασφαλισμένο δεν είναι μόνο δύσκολο να κλαπεί, αλλά ο δημόσιος χαρακτήρας του blockchain επιτρέπει επίσης την ταχεία αναγνώριση οποιασδήποτε κλοπής, καθώς σχετίζεται με την ασφάλεια του API.

Οποιοσδήποτε μπορεί να δει μια απόπειρα ελέγχου ταυτότητας για το Hydro smart contract, πράγμα που σημαίνει ότι οι ημέρες των πλατφορμών που διακυβεύονται για μήνες μπορεί να είναι παρελθόν. Οι hackers του API μπορούν τώρα να αποφευχθούν με μεγαλύτερη αμεσότητα λόγω της ικανότητας ανίχνευσης απροσδόκητων προσπαθειών εξουσιοδότησης σε πραγματικό χρόνο, από οπουδήποτε στον κόσμο.

Κίνδυνοι

Όπως όλες οι νέες τεχνολογίες, όπως οι πρώτες μέρες των κοινωνικών μέσων, των ηλεκτρονικών μηνυμάτων και των εφαρμογών συνεχούς ροής (που εξαρτώνται από τη σύνδεση μέσω τηλεφώνου), είναι σημαντικό η κεντρική αναπτυξιακή ομάδα να παρακολουθεί στενά τις νέες εξελίξεις στις ταχύτητες και τις ποσότητες συναλλαγών του Ethereum. Θα μπορούσατε να φανταστείτε το YouTube να προσπαθεί να ξεκινήσει το 1995; Ή το Instagram να προσφέρεται για πρώτη φορά στο Blackberry;

Κύριοι προγραμματιστές του Ethereum όπως ο Vitalik Buterin και ο Joseph Poon πρότειναν να αναβαθμιστεί στο πρωτόκολλο Ethereum το Plasma: Scalable Autonomous Smart Contracts :

> **Το πλάσμα είναι ένα προτεινόμενο πλαίσιο για την παροχή κινήτρων και την αναγκαστική εκτέλεση smart contracts, το οποίο είναι κλιμακωτό για ένα σημαντικό ποσοστό αναβαθμίσεων κατάστασης ανά δευτερόλεπτο (ενδεχομένως δισεκατομμύρια), επιτρέποντας στο blockchain να αντιπροσωπεύει σημαντικό αριθμό αποκεντρωμένων χρηματοπιστωτικών εφαρμογών παγκοσμίως. Αυτά τα smart contracts είναι κίνητρα για να συνεχίσουν να λειτουργούν αυτόνομα μέσω των network transaction fees (τελών συναλλαγής δικτύου), τα οποία τελικά εξαρτώνται από το υποκείμενο blockchain (π.χ. Ethereum) για την επιβολή μεταβατικών μεταβολών κατάστασης συναλλαγών.**

Άλλοι, όπως το The Raiden Network, πρότειναν μια λύση απομάκρυνσης από την αλυσίδα(off-chain) που σχεδιάστηκε για να τροφοδοτεί ταχύτερες συναλλαγές και χαμηλότερα fees (τέλη). Αυτή τη στιγμή, το Raindrop θα ασκήσει πολύ ελάχιστη πίεση στο πλαίσιο του Ethereuem, επομένως η επεκτασιμότητα είναι ένας πολύ μικρός κίνδυνος για την επιτυχία της τεχνολογίας.

Συμπέρασμα

Η αμετάβλητη λειτουργία ενός public blockchain προσφέρει νέους τρόπους για την ενίσχυση της ασφάλειας των ιδιωτικών συστημάτων όπως τα API.

Αυτό το έγγραφο έδειξε τρία σημαντικά πράγματα:

1. Τα public blockchains μπορούν να προσθέσουν αξία στις χρηματοπιστωτικές υπηρεσίες.
2. Το Hydro Raindrop μπορεί να ενισχύσει την ασφάλεια των ιδιωτικών συστημάτων.
3. Υπάρχουν άμεσες εφαρμογές του Hydro Raindrop εντός της πλατφόρμας Hydrogen API.

Η ομάδα Hydro πιστεύει ότι το πλαίσιο που έχει τεθεί μπορεί να είναι η τυποποιημένη υποδομή ασφάλειας για ένα νέο μοντέλο υβριδικών-ιδιωτικών δημόσιων συστημάτων, το οποίο θα ωφελήσει όλους τους φορείς του κλάδου των χρηματοπιστωτικών υπηρεσιών και πέραν αυτών.

Πηγές:

Ethereum; Merkling in Ethereum
Trend Micro; What Do Hackers Do With Your Stolen Identity?
Javelin Strategy & Research; *The 2017 Identity Fraud Study*
Symantec; *Internet Security Threat Report*
Risk Based Security; *2016 Data Breach Trends – Year in Review*
Thales; *2017 Thales Data Threat Report – Financial Services Edition*
Apache.org; Apache Struts 2 Documentation - S2-052
Joseph Poon and Vitalik Buterin; Plasma: Scalable Autonomous Smart Contracts